日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: １９９８年　５月１２日

出願番号
Application Number: 平成１０年特許願第１２９２１４号

出願人
Applicant (s): ソニー株式会社

１９９９年　３月１９日

特許庁長官
Commissioner,
Patent Office 伴佐山建志

【書類名】　特許願

【整理番号】　9800081404

【提出日】　平成10年 5月12日

【あて先】　特許庁長官　殿

【国際特許分類】　H04B　7/00

【発明の名称】　データ伝送制御方法及びデータ伝送システム

【請求項の数】　24

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　原　和弘

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代表者】　出井　伸之

【代理人】

【識別番号】　100067736

【弁理士】

【氏名又は名称】　小池　晃

【選任した代理人】

【識別番号】　100086335

【弁理士】

【氏名又は名称】　田村　榮一

【選任した代理人】

【識別番号】　100096677

【弁理士】

【氏名又は名称】　伊賀　誠司

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ伝送制御方法及びデータ伝送システム

【特許請求の範囲】

【請求項１】　通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの伝送制御を行うデータ伝送制御方法において、

上記データ送信手段から上記データ受信手段へのデータの伝送に使用する第１の通信経路を介して、上記データ送信手段において暗号化されたデータを上記データ受信手段に送信し、

上記第１の通信経路よりもデータ伝送容量の小さく、上記データ受信手段から上記データ送信手段へのデータの伝送にも使用される第２の通信経路、及び上記第１の通信経路の内の少なくとも上記第２の通信経路を介して、上記データ送信手段から送信される上記暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報を上記データ受信手段に送信すること

を特徴とするデータ伝送制御方法。

【請求項２】　上記第２の通信経路は、上記データ送信手段と上記データ受信手段との間を双方向通信可能にする通信回線であること

を特徴とする請求項１記載のデータ伝送制御方法。

【請求項３】　上記データの暗号化は、上記データ送信手段におけるデータの暗号化を暗号鍵を用いて行い、当該データ送信手段から伝送された当該暗号化されたデータの上記データ受信手段における復号化を当該暗号化に使用した暗号鍵と同じ復号鍵を用いて行う共通鍵方式によること

を特徴とする請求項１記載のデータ伝送制御方法。

【請求項４】　上記暗号鍵及び上記復号鍵は、情報データを暗号化及び復号化するためのセッション鍵であること

を特徴とする請求項３記載のデータ伝送制御方法。

【請求項５】　上記データ送信手段及び上記データ受信手段は、データ受信手段固有のマスター鍵を有し、

上記データ送信手段は、上記マスター鍵を用いて上記セッション鍵を暗号化して、上記第１の通信経路又は上記第２の通信経路を経由させて上記暗号化したセ

ッション鍵を上記データ受信手段に伝送し、

上記データ受信手段は、上記マスター鍵を用いて、受信した上記暗号化されたセッション鍵を復号化して取り出すこと

を特徴とする請求項４記載のデータ伝送制御方法。

【請求項６】　上記データ送信手段は、特定の情報データの受信が許可される全てのデータ受信手段に対応させて上記セッション鍵を所持し、

上記データ送信手段は、上記特定の情報データの受信が許可されるデータ受信手段に上記セッション鍵を予め伝送しておくこと

を特徴とする請求項５記載のデータ伝送制御方法。

【請求項７】　上記第１の通信経路は、上記データ送信手段から上記データ受信手段への片方向通信のみ可能な衛星回線であり、

上記第２の通信経路は、データ送信手段とデータ受信手段の間で双方向通信可能な通信回線であること

を特徴とする請求項１記載のデータ伝送制御方法。

【請求項８】　暗号化を施してデータを送信するデータ送信手段と、

データ送信手段から上記暗号化が施されたデータが伝送されるデータ受信手段と、

上記データ送信手段から上記データ受信手段へのデータの伝送に使用する第１の通信経路と、

上記データ受信手段から上記データ送信手段へのデータの伝送にも使用され、上記第１の通信経路よりもデータ伝送容量の小さい第２の通信経路と、

を有し、

上記データ送信手段から上記データ受信手段への暗号化したデータの伝送には、上記第１の通信経路を用い、

上記データ送信手段から上記データ受信手段への当該データ受信手段から送信する上記暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報の伝送には、少なくとも上記第２の通信経路を用いること

を特徴とするデータ伝送システム。

【請求項９】　上記データの暗号化は、上記データ送信手段におけるデータの暗号化を暗号鍵を用いて行い、当該データ送信手段から伝送された当該暗号化されたデータの上記データ受信手段における復号化を当該暗号化に使用した暗号鍵と同じ復号鍵を用いて行う共通鍵方式によること

を特徴とする請求項８記載のデータ伝送システム。

【請求項１０】　上記暗号鍵及び上記復号鍵は、情報データを暗号化及び復号化するためのセッション鍵であること

を特徴とする請求項９記載のデータ伝送システム。

【請求項１１】　上記データ送信手段及び上記データ受信手段は、データ受信手段固有のマスター鍵を有し、

上記データ送信手段は、上記マスター鍵を用いて上記セッション鍵を暗号化して、上記第１の通信経路又は上記第２の通信経路を経由させて上記暗号化したセッション鍵を上記データ受信手段に伝送し、

上記データ受信装置は、上記マスター鍵を用いて、受信した上記暗号化されたセッション鍵を復号化して取り出すこと

を特徴とする請求項１０記載のデータ伝送システム。

【請求項１２】　上記データ送信手段は、特定の情報データの受信が許可される全てのデータ受信手段に対応させて上記セッション鍵を所持し、

上記データ送信手段は、上記特定の情報データの受信が許可されるデータ受信手段に上記セッション鍵を予め伝送しておくこと

を特徴とする請求項１１記載のデータ伝送システム。

【請求項１３】　上記第１の通信経路は、上記データ送信手段から上記データ受信手段への片方向通信のみ可能な衛星回線であること

を特徴とする請求項８記載のデータ伝送システム。

【請求項１４】　通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの制御を行うものであって、上記データ送信手段でデータを暗号化し、当該暗号化したデータを上記データ受信手段に上記通信経路を介して伝送するデータ伝送制御方法において、

上記データ送信手段から上記データ受信手段へ伝送するデータを複数のプロト

コルに応じて多重にカプセル化するとともに、少なくとも一つの上記カプセル化に対して暗号化を施すこと

を特徴とするデータ伝送制御方法。

【請求項１５】　データのカプセル化は、上記データ受信手段への配信対象とするデータを第１のプロトコルに応じてカプセル化する第１のカプセル化工程と

、

上記第１のカプセル化工程においてカプセル化したデータを第２のプロトコルに応じてカプセル化する第２のカプセル化工程とにより行い、

上記第１のカプセル化工程は、上記データ受信手段への配信対象とするデータを全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化すること

を特徴とする請求項１４記載のデータ伝送制御方法。

【請求項１６】　上記付加情報部には、実データ部のデータの受信が許可されるデータ受信手段の宛先アドレス情報が含まれていること

を特徴とする請求項１５記載のデータ伝送制御方法。

【請求項１７】　上記データ送信手段は、当該データ送信手段においては情報データの暗号化に使用され、上記データ受信手段においては当該暗号化されて伝送されてきた情報データの復号化に使用されるセッション鍵を上記宛先アドレス情報に対応して所持し、

上記データ送信手段は、上記セッション鍵を上記宛先アドレス情報により受信が許可されるデータ受信手段に予め伝送しておくこと

を特徴とする請求項１６記載のデータ伝送制御方法。

【請求項１８】　上記データ送信手段から上記データ受信手段への上記セッション鍵の伝送は、上記データ送信手段と上記データ受信手段との間を片方向又は双方向通信可能としている通信回線により行うこと

を特徴とする請求項１７記載のデータ伝送制御方法。

【請求項１９】　上記第１のカプセル化工程は、実データ部に付加される上記宛先アドレス情報の上記付加情報部への格納を一意に決定し、当該宛先アドレス情報に対応される上記データ受信手段固有のマスター鍵により実データ部を暗号

化すること

を特徴とする請求項１５記載のデータ伝送制御方法。

【請求項２０】　上記付加情報部には、上記宛先アドレス情報の格納用に４８ビットの空間が用意されていること

を特徴とする請求項１６記載のデータ伝送制御方法。

【請求項２１】　上記第１のカプセル化工程により第１のプロトコルに応じてカプセル化されるデータは、インターネットプロトコル又はイーサネットプロトコルが採用されていること

を特徴とする請求項１５記載のデータ伝送制御方法。

【請求項２２】　通信経路を介してデータ送信手段からデータ受信手段に伝送するデータの制御を行うものであって、上記データ送信手段でデータを暗号化し、当該暗号化したデータを上記受信手段に上記通信経路を介して伝送するデータ伝送制御方法において、

暗号鍵を用いて上記データの上記暗号化を行うデータ暗号化工程と、

上記暗号化したデータに当該データの暗号化に使用した上記暗号鍵に関する暗号鍵情報を付加して、上記データ送信手段記から上記データ受信手段へ送信するデータ送信工程と、

上記データ受信手段において受信した上記暗号化されたデータを復号するための復号鍵を複数有し、頻繁に更新される前記復号鍵から上記暗号化されたデータに付加されている上記暗号鍵情報について選択される一の復号鍵により、上記暗号化されたデータを復号化するデータ復号化工程と

を有すること

を特徴とするデータ伝送制御方法。

【請求項２３】　上記複数の復号鍵は、受信される暗号化されたデータの復号化に現在利用可能とされる復号鍵及び受信される暗号化されたデータの復号化に次に使用される復号鍵であり、

上記データ復号化工程は、上記暗号鍵情報に基づいて上記現在利用可能な復号鍵を選択すること

を特徴とする請求項２２記載のデータ伝送制御方法。

【請求項２４】　上記暗号鍵及び上記復号鍵は、情報データを暗号化するためのセッション鍵であること

を特徴とする請求項２３記載のデータ伝送制御方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信回線を利用してデータ送信装置からデータ受信装置へのデータの伝送の制御を行うデータ伝送制御方法及びデータ伝送システムに関し、詳しくは、データ送信装置から伝送されるデータの受信を特定のデータ受信装置に限定する制御を行うデータ伝送制御方法及びデータ伝送システムに関する。

【０００２】

【従来の技術】

近年、データ送信装置から伝送されるデータを遠隔地に設置されている複数のデータ受信装置が受信可能とされるネットワーク型のデータ伝送システムが提供されている。例えば、衛星テレビジョン放送は、衛星回線を利用し、複数のデータ受信者に映像・音声情報を配信するいわゆるブロードキャスト的なデータ伝送システムを構築している。

【０００３】

また、ブロードキャスト的なデータ伝送システムには、ローカルエリアネットワーク（ＬＡＮ）として構築されるイーサネットが挙げられる。例えば、上記イーサネットのネットワークは、図１４に示すように、データを送信するデータ送信装置３５１と、データ送信装置３５１からネットワーク３５３を介してデータが伝送されるデータ受信装置３５２ａ，３５２ｂとから構成されている。例えば、このイーサネットにおいて、データ受信装置間の距離は、最大で数Ｋｍまでとされている。

【０００４】

このように構成されたデータ伝送システムにおいて、データ受信装置３５２ａにデータを送信したい場合は、データ送信装置３５１は、ネットワーク３５３に向けてデータを送信する。この際、送信されるデータには、データ受信装置３５

２ａを識別するための宛先アドレスが付加されて送信される。例えば、多くの宛先アドレスの情報を表現しようとした場合には、４８ビット必要とされる。

【０００５】

上記データ送信装置３５１からネットワーク３５３に送信されたデータは、データ受信装置３５２ａ及びデータ受信装置３５２ｂに受信され、各データ受信装置は、この受信したデータに付加されている宛先アドレスを参照して、自分宛のものであるかを判断する。例えば、イーサネットにおいて使用されるフレームフォーマットは、図１５に示すように構成され、宛先アドレス（Destination Address）４０１がデータの受信を行うデータ受信装置の宛先のアドレスを示す。

【０００６】

ここで、データ受信装置は、判断の結果が自分宛でないと判断したとき、そのデータを破棄する。このような手続きによって、データに自己の宛先アドレスが付加されているデータ受信装置３５２ａは、当該データを受信することができるが、データに自己の宛先アドレスが付加されていないデータ受信装置３５２ｂは、当該受信したデータを破棄することになる。

イーサネットにおけるデータ受信装置の受信処理は、図１６に示すようなフローチャートに従って実行される。

【０００７】

先ず、ステップＳ１０１において、データ受信装置は、ローカルエリアネットワークからデータが格納されたイーサネットフレームを受け取る。続くステップＳ１０２において、データ受信装置は、当該受け取ったイーサネットフレームから宛先アドレスを取り出す。そして、ステップＳ１０３において、データ受信装置は、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）であるか否かを判別する。ここで、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）であることを確認した場合には、データ受信装置は、当該イーサネットフレームをホストコンピュータに送信する。ここで、上記ユニキャストアドレスは、個人の宛先アドレスであって、上記マルチキャストアドレスは、複数のデータ受信装置が受信できるためのアドレ

ス、例えば、グループ単位でデータを受信するための宛先アドレスである。

【０００８】

一方、宛先アドレスが自分宛てのアドレス（ユニキャストアドレス）又は自分が参加しているアドレス（マルチキャストアドレス）の何れでもないことを確認した場合には、データ受信装置は、当該イーサネットフレームを破棄する。

【０００９】

上記宛先アドレスに基づいて行うデータの伝送方法によれば、標準通りに実装されたデータ受信装置であれば、宛先アドレスのないデータ受信装置は、データを受信することができないことになる。しかし、このようなデータ伝送方法においては、自己のアドレスを変更させるなどによりその判断機構を操作し、本来宛先アドレスとされていない、すなわちデータの送信対象とされていないデータ受信装置も他のデータ受信装置宛のデータを受信することが可能になり、これは他に知られたくないデータを送る際にはセキュリティの面で不安になる。

【００１０】

だが、イーサネットにおいては、同じネットワークに接続されるデータ受信装置間の距離や台数が制限されており、他のデータ受信装置にデータの内容を知られて問題が起きる状況は少ないと考えられる。例えば、イーサネットの１つの形態である１０BASE-５では、１つのセグメントのケーブルの長さは５００ｍまでであり、そこに繋げられるトランシーバ（データ受信装置）の数は１００台までと決められている。

【００１１】

一方、上述した衛星回線によりデータ伝送のネットワークが構築された場合には、同一のネットワークが日本全国よりも広い範囲に渡って設置されることが有り得る。例えば北海道にあるデータ受信装置に送ったデータを、沖縄県にあるデータ受信装置が受信することも可能になる。このように、衛星回線によるネットワークでは、広範囲にデータを伝送し、さらにデータを受信可能とされるデータ受信装置の台数が多くなることから意図しない相手にデータを知られてしまう可能性が多くなる。

【００１２】

よって、衛星回線などのブロードキャスト型の通信経路を用いてデータの伝送を行う場合には、データに何も加工を施さなければ、目的とするデータ受信装置以外のデータ受信装置においても、データの受信が可能になってしまう。この対策として、通信衛星を用いた現行のディジタル放送システムにおいては、送出するデータ（主に映像・音声情報）に暗号化を施してから衛星通信路上に伝送している。これに対応して、データ受信装置は、暗号化を解除する機能（復号化を行う機能）を有している。このようなデータ伝送方法により、予め視聴を許可されたデータ受信装置のみが復号化して視聴できるようになっている。これは、例えば、電気通信技術審議会７４号答申に準拠した方式であり、伝送フォーマットとしてＭＰＥＧ２（Moving Picture Experts Group Phase 2）のトランスポートストリームパケット（ＴＳパケット）を用いている。例えば、データ送信装置おけるデータの暗号化は、暗号鍵を用いて行い、上記データ受信装置における復号化では、上記暗号鍵に対応される復号鍵により行う。上記ＴＳパケットのフォーマットは、図１７に示すように構成され、ヘッダ部のＰＩＤ（Packet Identification）部４１１及びスクランブル制御部４１２により暗号鍵が特定される。ここで、例えば、暗号鍵は、セッション鍵Ksとワーク鍵Kwとがある。また、上記ＰＩＤ４１１は、１３ビットのデータであり、上記スクランブル制御部４１２は、２ビットのデータである。

【００１３】

上記ＴＳパケットによりデータの伝送を行う既存の衛星テレビジョン放送におけるデータ伝送システムは、例えば、図１８に示すように、データ送信装置５０１と、データ受信装置５１１とから構成されている。データ送信装置５０１は、各種暗号鍵により暗号化を行う暗号化ユニット５０２，５０３，５０４を有している。また、データ受信装置５１１は、各種復号鍵により復号化を行う復号化ユニット５１２，５１３，５１４と、資格判別ユニット５１５とを有している。

【００１４】

このように構成されるデータ伝送システムにおいて、先ずデータ送信装置５０１からデータ受信装置５１１へのワーク鍵Kwの伝送が行われる。すなわち、上記

データ送信装置５０１は、上記ＰＩＤ部４１１とスクランブル制御部４１２に対応したワーク鍵Kw５０６を予め作成する。そして、データ送信装置５０１は、当該ワーク鍵Kw５０６を、暗号化ユニット５０４において、マスター鍵５０７により暗号化し、データ受信装置５１１に伝送する。ここで、マスター鍵Kw５０７は、データ受信装置５１１固有のマスター鍵（復号鍵）５１８と同じ鍵とされている。データ送信装置５０１からデータ受信装置５１１へのワーク鍵Kwの伝送は、衛星回線を経由して行われる。

【００１５】

データ受信装置５１１では、マスター鍵Kw５０７により暗号化されたワーク鍵Kwを受信して、復号化ニット５１４において、当該データ受信装置５１１の固有のマスター鍵Km５１８により復号化する。そして、データ受信装置５１１は、復号して取り出したワーク鍵Kw５１７を上記ＰＩＤと対応させて保存する。このワーク鍵Kwは、データ送信装置５０１から送信される暗号化されたデータの復号化に使用される。

【００１６】

データ送信装置５０１からデータ受信装置５１１へのデータの送信については、上記データ送信装置５０１は、データのＴＳパケットのペイロード部分４１３を、暗号化ユニット５０２においてセッション鍵Ks５０５により暗号化し、また同時に当該セッション鍵Ks５０５を暗号化ユニット５０３においてワーク鍵Kw５０６により暗号化する。

【００１７】

データ受信装置５１１では、自分が復号可能なＰＩＤを持つＴＳパケットを受信した際には、まず送られてきたＴＳパケットのＰＩＤ部４１１を見て予め保存してあった上記ワーク鍵Kw５１７を取り出す。そして、データ受信装置５１１は、データ送信装置５０１からデータと共に送信されてきた暗号化されたセッション鍵Ksをその取り出したワーク鍵Kw５１７を用いて復号化する。それから、データ受信装置５１１は、その復号化して取り出したセッション鍵Ks５１６を用いて、ＴＳパケットのペイロード部４１３を復号化し、データを取り出す。

【００１８】

なお、視聴を許可されていないデータ受信装置にあっては、所定のワーク鍵Kwが送信されてきていないので、視聴したいＰＩＤに対応するワーク鍵Kwを所持することはない。よって、このようなデータ受信装置は、データ送信装置５０１から上記所定のワーク鍵Kwにより暗号化されて送信されてきたセッション鍵Ksを復号することができず、これにより、データ送信装置５０１から暗号化されて送信されてきたデータも復号することができない。よって、結局許可されていないデータ受信装置は、データを受信することはできるが復号化処理を行うことができないので、当該データを視聴できない。

【００１９】

このようにして、衛星回線を用いた放送システムでは、限定的なデータの伝送制御を実現している。なお、上述したような、放送システムに限られず、例えば、インターネットにおいても様々な限定的なデータの伝送制御方法がある。

【００２０】

例えば、インターネットに関しては、電子メールを暗号化して他者の盗聴や改竄を防ぐＰＧＰ（Pretty Good Privacy）及びＰＥＭ（Privacy Enhanced Mail）、又はＨＴＴＰ（Hyper Text Transfer Protocol）で電子商取引をする際などにクレジットカード番号を盗聴されないようにできるＳＳＬ（Secure Socket Layer）などが使われている。これらは暗号化方式を利用したり柔軟なデータ伝送制御ができることが特徴である。

【００２１】

また、ＩＰ（Internet Protocol）データグラムに対するより汎用のデータ伝送制御方法として、認証ヘッダ（Authentication Header:AH）や、暗号ペイロード（Encapsulationg Security Payload:ESP）などのＩＰＳＥＣと呼ばれる方式が標準化されている。

【００２２】

【発明が解決しようとする課題】

ところで、衛星回線を使用したテレビジョン放送については、次のようなことが問題とされる。

【００２３】

第１の問題点は、データ受信装置の限定範囲の種類が少ないことである。すなわち、暗号鍵を識別するための情報とされるＰＩＤ部及びスクランブル制御部が、図１７に示すように、それぞれ１３ビット及び２ビットしか用いていないため、最大でも１５ビット分（2^{15}=３２７６８通り）の限定しかできない。

【００２４】

第２の問題点は、利用するＰＩＤの数を増やすと、送信側のコストが増大することである。例えば、データ受信装置において、ＰＩＤの数にほぼ比例した台数のＭＰＥ２のエンコーダが必要になるため、ＰＩＤの数を増加させると、それだけデータ送信装置のコストが増大し、装置が大掛かりなものになってしまう。

【００２５】

第３の問題点は、衛星回線を利用したデータ伝送では、片方向の送信となるので、情報が各データ受信装置に正しく伝わったかどうかをデータ送信装置が知ることができない。これにより、例えば、データ受信装置がデータの受信を許可されているにもかかわらず、実際にはデータを受信することができないような事態が発生してしまう。だからといって、より確実に各種情報をデータ受信装置に送るには、時間が必要になり、これは、無駄が多く、柔軟なデータ伝送制御の妨げとなる。

【００２６】

第４の問題点は、上述したように、ＩＰデータグラムを伝送する場合は、データ送信装置でインターネットプロトコルの宛先アドレスからＰＩＤの対応付けを行わなくてはならなく、インターネットプロトコルとの親和性に関して問題がある。具体的には、ＩＰデータグラムの宛先アドレスは３２ビットあり、それよりビット長の短い１３ビットのＰＩＤに対応付けるのは難しい等の問題がある。さらに、インターネットで現在用いられている上記の方法では、第５の問題点として、ＰＧＰ、ＰＥＭ、ＳＳＬなどは、アプリケーション固有のデータ伝送制御であり、インターネットでのすべてのアプリケーションで共通の方式ではないということである。アプリケーション毎に制御方法を用意しなくてはいけないのでは、新しいアプリケーションができたときへの素早い対応が難しくなる。

【００２７】

第６の問題点としては、認証ヘッダや暗号ペイロードは、アプリケーションに依存していないが、既存のバージョンのインターネットプロトコル、例えばＩＰｖ４では対応しているネットワーク機器がほとんどないという問題がある。認証ヘッダや暗号ペイロードは、インターネットプロトコルの次期のバージョン、例えば、ＩＰｖ６では標準的に利用されるが、既存のインターネットでは使うことは実質的に困難とされている。

【００２８】

そこで、本発明は、上述の実情に鑑みてなされたものであり、データ送信装置からデータ受信装置へのデータの送信を安全に、さらに確実に行うことを実現可能にするデータ伝送制御方法及びデータ伝送システムの提供を目的とする。

【００２９】

【課題を解決するための手段】

本発明に係るデータ伝送制御方法は、上述の課題を解決するために、データ送信手段からデータ受信手段へのデータの伝送に使用する第１の通信経路を介して、データ送信手段において暗号化されたデータをデータ受信手段に送信し、第１の通信経路よりもデータ伝送容量の小さく、データ受信手段からデータ送信手段へのデータの伝送にも使用される第２の通信経路、及び第１の通信経路の内の少なくとも第２の通信経路を介して、データ送信手段から送信される暗号化されたデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報を上記データ受信手段に送信している。

【００３０】

このデータ伝送制御方法は、第１の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、少なくとも第２の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行う。

【００３１】

このデータ伝送制御方法により、第１の通信経路及び第２の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第２の通信経路により当該データ送信手段と当該データ受信

手段との間でのデータの送受信に関する情報に関して情報の交換を行う。

【００３２】

また、本発明に係るデータ伝送システムは、上述の課題を解決するために、データ送信手段からデータ受信手段へのデータの伝送に使用する第１の通信経路と、データ送信手段と上記データ受信手段との間を双方向通信可能にする第２の通信経路とを有し、データ送信手段からデータ受信手段への暗号化したデータの伝送には、第１の通信経路を用い、データ送信手段からデータ受信手段への当該データ送信手段から送信する所定のデータを特定のデータ受信手段のみが受信するためのデータ限定伝送制御情報の伝送には、少なくとも第２の通信経路を用いる。

【００３３】

このような構成を有するデータ伝送システムは、第１の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、第２の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行う。

【００３４】

このデータ伝送システムにより、第１の通信経路及び第２の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第２の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行う。

【００３５】

また、本発明に係るデータ伝送制御方法は、上述の課題を解決するために、データ送信手段からデータ受信手段へ伝送するデータを複数のプロトコルに応じて多重にカプセル化するとともに、少なくとも一つのカプセル化に対して暗号化を施す。

【００３６】

このデータ伝送制御方法により、データ送信手段からデータ受信手段に送信されるデータが複数のプロトコルによって多重化されてカプセル化される。

【００３７】

これにより、所定のプロトコルを保ったままデータの送信が可能になり、すなわち、例えば、所定のプロトコルとの互換性を保ったままデータの送信が可能になり、さらに、所定のデータを格納するための空間が確保することができるプロトコルによりカプセル化することにより、各種情報を格納するためのデータ空間が確保される。さらに、暗号化が施されることにより、データの安全性が保たれる。

【００３８】

また、本発明に係るデータ伝送制御方法は、上述の課題を解決するために、暗号鍵を用いてデータの暗号化を行うデータ暗号化工程と、暗号化したデータに当該データの暗号化に使用した上記暗号鍵に関する暗号鍵情報を付加して、データ送信手段記からデータ受信手段へ送信するデータ送信工程と、データ受信手段において受信した暗号化されたデータを復号するための復号鍵を複数有し、頻繁に更新される前記復号鍵から上記暗号化されたデータに付加されている上記暗号鍵情報にづいて選択される一つの復号鍵により、暗号化されたデータを復号化するデータ復号化工程を有する。

【００３９】

このデータ伝送制御方法は、データ暗号工程において暗号鍵により暗号化されたデータに当該データの暗号化に使用した暗号鍵に関する暗号鍵情報を付加して、データ送信工程により、データ送信手段からデータ受信手段へ当該データを送信する。そして、データ受信手段において、データ復号化工程により、受信した暗号化されたデータを復号するための複数の復号鍵であって、頻繁に更新される復号鍵から、暗号化されたデータに付加されている暗号鍵情報にづいて選択した一つの復号鍵により、当該暗号化されたデータの復号化を行う。

【００４０】

このデータ伝送制御方法により、データ送信手段は、暗号鍵によるデータの暗号化を行い、データ受信手段は、受信した暗号化されているデータを復号鍵により復号化する。さらに、データ受信手段は、頻繁に変更される復号鍵から一の復号鍵を選択して、当該選択した復号鍵により復号化を行う。このとき、データ受

信手段は、当該暗号化されたデータとともに送信されてくる暗号鍵情報に基づいて複数の復号鍵から一つの復号鍵を選択する。

【００４１】

【発明の実施の形態】

以下、本発明の実施の形態について図面を用いて詳しく説明する。この実施の形態は、本発明に係るデータ伝送システムを、衛星回線を介してデータ送信装置から伝送されるデータの受信を特定のデータ受信装置に限定する制御を行うデータ伝送システムに適用したものである。

【００４２】

上記データ伝送システムは、図１に示すように、通信経路とされる衛星回線４ａ、専用線７、電話回線８、及び双方向の通信経路９を介してデータ送信装置２からデータ受信装置３ａ，３ｂ，３ｃに伝送するデータの制御を行うものであって、上記データ送信装置２でデータを暗号化し、当該暗号化したデータをデータ受信装置３ａ，３ｂ，３ｃに通信経路を介して伝送するデータ伝送システムである。

【００４３】

このデータ伝送システム１は、データ送信装置２からデータ受信装置３ａ，３ｂ，３ｃへのデータの伝送に使用する第１の通信経路とされる通信衛星４を利用した通信経路４ａと、データ送信装置２とデータ受信装置３ａ，３ｂ，３ｃとの間を双方向通信可能にする第２の通信経路である専用線７、電話回線８、及び双方向の通信経路９とを有している。そして、データ伝送システム１は、データ送信装置２からデータ受信装置３ａ，３ｂ，３ｃへの暗号化したデータの伝送には、上記第１の通信経路を用い、データ送信装置２からデータ受信装置へのデータ限定伝送制御情報の伝送には、上記第２の通信経路を用いている。そして、データ伝送システム１は、インターネットと接続されている。

【００４４】

ここで、データ限定伝送制御情報とは、上記データ送信装置２から送信する所定のデータを特定のデータ受信装置のみが受信するための情報である。すなわち、データ伝送制御情報とは、特定のデータ受信装置のみが所定のデータの受信が

許可されるための情報である。

【００４５】

上記データ送信装置２は、上記各通信回線を利用してデータ受信装置３ａ，３ｂ，３ｃへの各種データの配信を行う。データ受信装置３ａ，３ｂ，３ｃは、各通信回線から伝送されてくるデータを受信する。なお、図１には、データ受信装置３ａ，３ｂ，３ｃを３台として示しているが、実際には数百台から数万台のデータ受信装置が存在して当該データ伝送システム１を構成している。

【００４６】

このデータ送信装置２とデータ受信装置３ａ，３ｂ，３ｃ（なお、以下の説明では、データ受信装置３ａ，３ｂ，３ｃについて特定する必要がない場合には、単にデータ受信装置３という。）との間でデータの送受信を可能にする通信経路については、次のように構成されている。

【００４７】

上記衛星回線４ａは、約３０Mbpsの帯域を持ったＫｕバンドの片方向の回線を想定する。この衛星回線４ａにより、例えば、日本全国に分布されているデータ受信装置に対して、データ送信装置２からのデータの伝送を同時期に行うことができる。

【００４８】

双方向の通信経路９は、データ送信装置２とデータ受信装置３との間で、衛星回線４ａとは別に設けた通信経路であって、データ送信装置２とデータ受信装置３との間でので双方向通信を可能にするものである。ここでは、双方向の通信経路９は、インターネットでの通信に用いる汎用の通信経路を想定している。

【００４９】

専用線７は、データ送信装置２とデータ受信装置３とを直接接続している通信手段である。

【００５０】

上記インターネット６は、いわゆる映像情報、音楽情報等の各種情報を提供するものであって、上記インターネットサービスプロバイダ５により、インターネット６とデータ受信装置３とは通信可能に接続されている。ここでデータ送信送

信装置２は、インターネット６に接続されている。

【００５１】

なお、上述したようにデータ送信装置２とデータ受信装置３との間でデータの送受信を可能にする専用線７、電話回線８、及び双方向の通信経路９は、衛星回線４ａほど大容量の帯域ではなく、数Kbpsから数百Kbps程度が通常の帯域とされる。

【００５２】

上記データ伝送システム１は、所定のデータを特定のデータ受信装置においてのみ受信することを可能にするいわゆるデータ限定受信システムとしても構築されており、例えばデータ受信装置３ａのみにデータを伝送するといった個別配信（ユニキャスト型データ配信）、又は例えばデータ受信装置３ａ，３ｂとからなる受信グループにのみデータを伝送するといったグループ宛の同報配信（マルチキャスト型データ配信）、又は全てのデータ受信装置３ａ，３ｂ，３ｃに同時にデータを伝送するといった一斉配信（ブロードキャスト型配信）等の配信形態が可能とされて構成されている。

【００５３】

次に、このデータ伝送システム１において、データ送信装置２からデータ受信装置３へのデータの伝送について説明する。データ送信装置２からデータ受信装置３へ伝送されるデータは、図２に示すように、データのカプセル化が施されている。このカプセル化は、データを伝送するデータ送信装置２において行われる処理であって、第１のカプセル化工程により、データ受信装置３への配信対象とされるデータを第１のプロトコルによりカプセル化し、第２のカプセル化工程により、上記第１のプロトコルによりカプセル化したデータを第２のプロトコルによってカプセル化する。ここで、カプセル化とは、データ自体に対して加工を施すことなく、当該データ自身を通信プロトコルにより規定された伝送フォーマットに基づいて構成されるカプセル（パケット又はフレーム等）に入れ込むことをいい、このカプセル化によりデータの伝送制御が可能になる。

【００５４】

上記第１のカプセル化工程では、データ受信装置３への配信対象とするデータ

の全体を含む実データ部に当該実データ部に関する付加情報部を付加してカプセル化するとともに、上記実データ部については暗号化して上記カプセル化を行う。以下に詳しく説明する。

【００５５】

ＩＰ（Internet Protocol）データグラム１０１は、図２中（ａ）に示すように、インターネットプロトコルに則して構成されているデータである。このＩＰデータグラム１０１は、上記データ受信装置３への配信対象とされるデータを格納して構成されている。そして、ＩＰデータグラムのヘッダ部には、例えば、インターネット上において使用される宛先を識別するための送信先アドレス（Destination　Address）が付加されている。

【００５６】

なお、ＩＰデータグラム１０１の部分は、インターネットプロトコルとして構成されることに限定されるものではなく、イーサネットプロトコルを採用して構成されてもよい。

【００５７】

そして、データ送信装置２は、図２中（ｂ）から図２中（ｄ）に示すように、データを上記第１のプロトコルによりカプセル化する。例えば、第１のプロトコルとしては、ＤＶＢ（Digital Video Broadcasting）のMultiprotocol Encapsulationを採用している。

【００５８】

先ず、データ送信装置２は、第１のプロトコルによるデータのカプセル化を、図２中（ｂ）に示すように、ＩＰデータグラムに対してパディングを行い（パディング部１０２を付加する）、データ部の長さを６４ビットの整数倍にする。例えば、ＩＰデータグラム１０１の末尾に０ビット～６３ビット長のパディングを行い、パディングするビットは、すべて１とする。このパディングにより、所定のデータ長さにすることができ、これは、上記セクションのデータ部を暗号化する際に、データ部の長さが６４ビットの整数倍の方が都合が良いからである。以後、第１のプロトコルのフォーマットによって構成されるデータ部分をセクションと呼ぶことにする。

【００５９】

次に、データ送信装置２は、パディング１０２が付加されたセクションを、図２中（ｃ）に示すように、暗号化する。ここで、暗号化は、暗号鍵によって行うもので、暗号鍵は、上記データ受信装置３に対して配信の対象とされる情報について暗号化するために使用される後述するセッション鍵である。また、暗号化の方式としては、Triple-DESのような共通鍵方式のブロック暗号化を用いる。このTriple-DES方式の暗号化は、公開鍵方式の中でも強力な暗号方式であり、ハードウェアによる実装で高速化も容易とされる。これにより、３０Mbps程度の高速な暗号化にあっても、公開鍵方式の暗号化とは異なり、処理時間がかかってデータの伝送が間に合わなくなることを防止することができる。

【００６０】

そして、データ送信装置２は、図２中（ｄ）に示すように、暗号化されたセクションデータ部１０４に、セクションヘッダ部１０３及びエラー検出のために使用されるテイラ部１０５を付加する。

【００６１】

ここで、上記暗号化されたセクションデータ部１０４は、ＭＡＣ（Media Access Control）フレーム化されて構成されている。このＭＡＣフレーム化により、データ部にＭＡＣヘッダが付加され、このＭＡＣヘッダ部を参照することにより、当該フレーム化されて格納されているデータの宛先の制御が容易となされるようになる。具体的には、ＭＡＣフレームには、当該ＭＡＣフレーム化されたデータの受信が許可されているデータ受信装置の宛先アドレスが格納されている。

【００６２】

上記セクションヘッダ部１０３は、宛先アドレスを格納する部分であって、４８ビットの宛先アドレスが格納されるようにデータ空間が確保されている。具体的には、上記セクションヘッダ部１０３においてＭＡＣヘッダ部を構成して、宛先アドレスが格納されている。このセクションヘッダ部１０３に４８ビットにより表現される宛先アドレスを格納できる空間を設けることにより、上記第１の問題点とされていた、データ受信装置の限定範囲の種類が少ないことを解消することができる。すなわち、暗号鍵を識別するための多くの情報を格納することがで

きるようになる。さらに、上記第４の問題点とされていた、ＩＰデータグラム１０１を伝送する際に、インターネットプロトコルの宛先アドレスから後述するパケットＩＤの対応付けを行わなくもよくなり、インターネットプロトコルとの親和性を得ることができる。

【００６３】

また、上記テイラ部１０５は、ＣＲＣ（Cyclic Redundancy Checking、巡回冗長検査）によってコード化されている。ＣＲＣは、ＭＡＣフレーム化されたデータを受信したデータ受信装置３が、当該ＭＡＣフレームが正しく衛星回線において伝送されているかを検査するためのものである。例えば、ＣＲＣは、３２ビットによってコード化されている。

【００６４】

以上が第１のプロトコルによる配信対象とされるデータのカプセル化であって、次に、この第１のプロトコルによってカプセル化されたデータを、第２のプロトコルによってカプセル化させる処理について説明する。

【００６５】

第２のプロトコルによるカプセル化は、上記第１のプロトコルによってカプセル化されたデータを、複数のパケットに分割することにより実行されるカプセル化である。ここで、第２のプロトコルは、ＴＳ（Transport Stream）パケット化によるものである。ＭＰＥＧ２（Moving Picture Experts Group Phase 2）によって規格されているものであって、オーディオ、ビデオ信号やデータのような多種類のデータが多重化されて、大容量のディジタル回線で伝送することが可能になる。この第２のプロトコルにより、図２中（ｅ）乃至図２中（ｇ）に示すように、カプセル化されて、複数のＴＳパケット１０６，１０７，１０８に分割される。ここで、ＴＳパケット１０６，１０７，１０８は、ＴＳヘッダ部H_{TS}と、ＴＳペーロード部Ｐとによって構成され、上記ＴＳペイロード部Ｐには、分割されて上記第１のプロトコルによってカプセル化されたデータが格納される。そして、ＴＳパケットのＴＳヘッダ部H_{TS}には、上記図１７に示すような、パケットＩＤ（ＰＩＤ）部及びスクランブル制御部によって構成される。なお、従来においては、このＰＩＤ部及びスクランブル制御部に宛先アドレスが書き込んでいるこ

とにより、宛先アドレス情報が制限される等の問題があったが、本実施の形態においては、上述したように、宛先アドレスをセクションヘッダ部１０３に書き込むことにより、これを解消している。

【００６６】

以上が第２のプロトコルによるカプセル化であり、よって、データ送信装置２は、データ受信装置３への配信対象とされるデータ（ＩＰデータグラム）を第１のプロトコル及び第２のプロトコルによって多重にカプセル化して、通信衛星４への当該データの伝送を行っている。

【００６７】

このように、ＴＳパケットとセクションの２つのレベルにおいてそれぞれ独立なデータ限定伝送制御を行っているので、上記第２、第５、及び第６の問題点が解消される。

【００６８】

すなわち、上記第２の問題点とされていた、利用するＰＩＤを増加することなく、暗号鍵について多くの情報を確保することができる。

【００６９】

また、上記第５の問題点とされていた、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応がでいるようになる。

【００７０】

さらに、第６の問題点とされていた、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【００７１】

なお、上述したようなＩＰデータグラムをカプセル化してデータ受信装置３に送信する方法は、衛星回線４ａを介して行う際のものであり、双方向の通信経路９にあっては、特殊なカプセル化は行わず、通常のインターネットと同様の方式でＩＰデータグラムを伝送する。

【００７２】

次に、データ送信装置２において行う暗号鍵によるデータの暗号鍵及びデータ受信装置３において行う暗号化されているデータの暗号鍵（復号鍵）による復号

化について説明する。ここで、データ送信装置２及びデータ受信装置３は、図３に示すように構成され、データ送信装置２とデータ受信装置３とは、上記図１に示すような通信経路により接続されている。ここで、データ送信装置２からデータ送信装置３へのデータ伝送を第１のプロトコル（セクション）において行い、従来として説明した上記図１８については、本発明の実施の形態でいう第２のプロトコル（ＴＳパケット）により行っている。すなわち、本発明実施の形態である図３と従来のものとされる図１８とに示されるデータ送信装置及びデータ受信装置を比較すると、本発明に係る実施の形態とされるところのデータ送信装置とデータ受信装置において暗号化及び復号化に使用される鍵のレベル、すなわち、鍵の使用個数が１つ少なく、セッション鍵Ks２４とマスター鍵Km２５の２レベルになっている。

【００７３】

ここで、セッション鍵Ks２４は、上記データ送信装置２及び上記データ受信装置３が共に所持しているデータの暗号化／復号化に使用する鍵であり、いわゆる共通鍵方式が採用されている。なお、便宜的にデータ送信装置３が所持する方のセッション鍵Ksをセッション鍵Ks３４とする。

【００７４】

すなわち、データ送信装置２は、セッション鍵Ks２４により、特定のデータ受信装置に対して送る情報データを暗号化する。また、データ受信装置３は、配信されてきた暗号化されたデータをセッション鍵Ks３４により復号化して意味のある情報として取り出す。

【００７５】

そして、セッション鍵Ks２４，３４は、一定時間毎に更新される暗号鍵であって、例えば、日毎、時間毎、分毎に変化する。よって、ある時点でのセッション鍵Ks２４を盗聴者が知ったとしても、有効とされる期間が一定期間であることから、そのセッション鍵Ks２４により一定期間しかデータの盗聴をすることができない。このセッション鍵Ksの更新については、後述する。

【００７６】

このセッション鍵Ks２４により、図２内（ｃ）に示すセクションのデータ部は

、上記Triple-DESにより暗号化される。

【００７７】

マスター鍵Km２５は、上記セッション鍵Ksと同様に、データ送信装置２及びデータ受信装置３が共に所持している暗号鍵であって、各データ受信装置３Ａ，３Ｂ，３Ｃに固有のものである。なお、便宜的にデータ送信装置３側の所持するマスター鍵Kmをマスター鍵Km３５とする。

【００７８】

このマスター鍵Ks２５は、データ送信装置２とデータ受信装置３と間を送信処理されるようなことはなく、すなわち、通信経路上に存在する場合はなく、これによりいかなる手段によっても他人によって知ることができない暗号鍵とされている。

【００７９】

このマスター鍵Kmは、セッション鍵Ksをデータ送信装置２からデータ受信装置３に送信する際に、セッション鍵Ksを暗号化／復号化するために用いられる。すなわち、データ送信装置２は、マスター鍵Km２５によりセッション鍵Ks２４を暗号化してデータ受信装置３に予め伝送しておく。データ受信装置３は、受信した暗号化されているセッション鍵Ks２４を、当該データ受信装置３が所持しているマスター鍵Kmによって復号化して取り出す（セッション鍵Ks３４として取り出す）。

【００８０】

このマスター鍵Kmによる暗号化及び復号化により、セッション鍵Ksは、データ送信装置２からデータ受信装置３へ伝送する間に盗聴者が存在している場合であっても、知られるようなことはない。

【００８１】

そして、データ受信装置３は、復号化したセッション鍵Ksにより、当該セッション鍵Ksにより暗号化されて伝送されてくる情報データの復号化を行い、情報データを意味のある情報として取り出す。

【００８２】

なお、このマスター鍵Kmによるセッション鍵Ksの暗号化／復号化についても、

上記Triple-DESに基づいて行うが、公開暗号方式を採用することもできる。これは、公開暗号方式は、鍵の暗号化及び復号化がデータの暗号化/復号化とは異なり高速性を要求されないこと、安全性を確保することができるからである。

【００８３】

また、マスター鍵Km２５は、セッション鍵Ks２４と異なり、時間と共に変化することはない。

【００８４】

ここで、セッション鍵Ks２４の変更について説明する。セッション鍵Ksの変更については、データ送信装置２が能動的に行うものとし、マスター鍵Km２５で暗号化したセッション鍵Ks２４（以下、マスター鍵Kmにより暗号化されたセッション鍵Ksを、暗号化されたセッション鍵Km(Ks)という。）の伝送もデータ送信装置２が能動的に行うものとする。

【００８５】

また、双方向通信経路９を利用することにより、データ受信装置３の側から能動的にセッション鍵Ksの要求を行うこともできる。これにより、各データ受信装置３ａ，３ｂ，３ｃは、素早く確実に必要なセッション鍵Ks２４をデータ送信装置３から取得することができる。具体的には、新たにデータ受信装置３がこのデータ伝送システム１に加わる場合、障害によりこの系から外れていたデータ受信装置３が障害から復旧して再びこのデータ伝送システムに加わる場合、またデータ受信装置３においてセッション鍵Ksが正しく受信出来なかった場合などには、データ受信装置３の側から能動的にセッション鍵Ksの要求を行うことにより、各データ受信装置３ａ，３ｂ，３ｃは素早く確実に必要なセッション鍵Ks２４を取得することができる。例えば、上述したような障害復旧やセッション鍵Ksの更新の管理は、データ送信装置２及びデータ受信装置３内にあるＣＡ（Conditional Access）管理ユニット２３，３３により行い、両者が双方向に通信を行って制御情報のやりとりを行う。

【００８６】

よって、上記第３の問題点とされていた、衛星回線のみをデータ伝送システムに組み込むことによる弊害、例えば、情報が各データ受信装置に正しく伝わった

かどうかをデータ送信装置が知ることができない等といった問題を解決することができる。

【００８７】

また、データ送信装置２からデータ受信装置３へのセッション鍵Ksの伝送については、片方向通信経路とされる衛星回線４ａに行ってもよく、双方向の通信経路９によって行ってもよい。

【００８８】

セッション鍵Ksの更新手順については、図４に示すようなフローチャートに従って実行される。

【００８９】

まず、ある時点において、データ受信装置３は、セッション鍵Ks３４として、セッション鍵Ks_evenと、セッション鍵Ks_oddの２つを保持している。データ受信装置３は、このようにセッション鍵Ksを２つ所持することにより、このセッション鍵Ks_even又はセッション鍵Ks_oddの何れかを使用して、データ送信装置２から送信されてくる情報データの復号化を行う。

【００９０】

ここで、現在使っているセッション鍵Ksがどちらであるかは、上記図２に示すセッションヘッダ部１０３に情報として書き込まれている。例えば、セクションヘッダ部１０３は、図５に示すように、テーブルＩＤ（table_id）、ＭＡＣアドレス部（MAC_address_1,MAC_address_2,MAC_address_3,MAC_address_4,MAC_address_5,MAC_address_6）と、セクション情報部（section_length,section_number,last_section_number）、ｓｓｉ（section_syntax_indicator）、ｐｉ（private_indicator）、ｒｓｖｄ（reserved）、ｐｓｃ（payload_scramble_indicator）１１１、ａｓｃ（address_scramble_indicator）、ＬＳｆ（LLC_SNAP_flag）、及びｃｎｉ（current_next_indicator）によって構成さている。ここで、ｐｓｃ１１１が現在使っているセッション鍵Ksがどちらであるかの情報を示す。例えば、上記ｐｓｃ１１１は、２ビットの情報であり、例えば、ｐｓｃの上位ビットが「０」のときは、セッション鍵Ks_evenが使用されていることを示し、ｐｓｃの女医うビットが「１」のときには、セッション鍵Ks_oddが使用されていること

を示す。

【００９１】

上述したような使用されているセッション鍵Ksの判断をステップＳ１において行った後、データ受信装置３は、ステップＳ２において、タイマーでトリガをかけ、セッション鍵Ksの更新タイミングを知る。

【００９２】

続いて、データ受信装置３は、ステップＳ３において、ＭＡＣアドレスとセッション鍵Ksの対応表にある現在のセッション鍵Ksのフラグを更新する。データ受信装置３は、例えば、図６のＭＡＣアドレスとセッション鍵Ksの対応表を有しており、この対応表を参照して、現在のセッション鍵Ksのフラグ１１２を更新する。この更新処理により、上記のｐｓｃ１１１の上位１ビットが反転する。例えば、ｐｓｃの上位ビットが「０」に反転される。

【００９３】

そして、データ受信装置３では、ステップＳ４において、そのｐｓｃに基づいてそのセクションに含まれているＩＰデータグラムの復号化を行う。すなわち、ｐｓｃの上位ビットが「０」とされた場合には、データ受信装置３は、これまで使用していたセッション鍵Ks_odd（ｐｓｃの上位ビットが「１」のとき使用されるセッション鍵Ks）から変更して、セッション鍵Ks_evenにより復号化を行う。また、ｐｓｃの上位ビットが「１」とされた場合には、データ受信装置３は、これまで使用していたセッション鍵Ks_even（ｐｓｃの上位ビットが「０」のとき使用されるセッション鍵Ks）から変更して、セッション鍵Ks_oddにより復号化を行う。

【００９４】

そして、次のセッション鍵Ksの切替えのタイミングまでの間に、ステップＳ５において、データ送信装置２からデータ受信装置３に対して、次のセッション鍵Ksをマスター鍵Km２４により暗号化して転送する。

【００９５】

ここで、 暗号化されたセッション鍵Km(Ks)の転送は、衛星回線４ａ又は双方向の通信回線９を使って伝送する。例えば、伝送の際のプロトコルについては、

応答の伴うプロトコルを用い、例えば、ＴＣＰ／ＩＰ（Transmissiom Control Protcol／Internet Protocol）を使用する。これにより、データ送信装置２からデータ受信装置３へのセッション鍵Ksの伝送が確実に行われる。

【００９６】

そして、この転送処理の間に、ステップＳ６において、データ受信装置３は、図６に示すＭＡＣアドレスのセッション鍵Ksの対象表の更新を行う。すなわち、以前使用していたセッション鍵Ksを、新しいセッション鍵Ksに書き換える処理を行う。

【００９７】

その後、ステップＳ７において、データ受信装置３は、対象とするデータ受信装置３に次のセッション鍵Ksが保持されたかを確認した後に、ステップＳ８に進み、次のセッション鍵Ksに切り替える。ここで、ステップＳ８以降ステップＳ１３までの処理は、ｐｓｃの上位ビットが「１」とされて、セッション鍵Ks_oddを復号化に使用するときの処理であって、上記ステップＳ７から進む処理であり、また、上記ステップＳ１において、データ受信装置３が現在のセッション鍵Ksがセッション鍵Ks__even（ｐｓｃの上位ビットが「０」）とされたときに実行される処理でもある。

【００９８】

上述したような手順により、データ送信装置２は、確実に更新されるセッション鍵Ksをデータ受信装置３に届けることができ、データ受信装置２では、２つ所持するセッション鍵Ksを切替えを瞬時に行い、データの取りこぼしもなくセッション鍵Ksによる復号化を実現することができる。なお、伝送処理時間の許す範囲で、セッション鍵Ｋｓ２４の更新頻度は柔軟に変更することが可能である。

【００９９】

以上のようにセッション鍵Ksがデータ受信装置３において、逐次変更されている。データ受信装置３は、このように変更されるセッション鍵Ksによって、共に転送されてくる情報データの復号を行っている。

【０１００】

次にデータ送信装置２がデータを送信するまでの手順、及びデータ受信装置が

データを受信したときの手順について説明する。データ送信装置２がデータを送信するまでの手順については、例えば、図７に示すフローチャートに従って実行している。そして、データ受信装置３がデータを受信してからの手順については、例えば、図９に示すフローチャートに従って実行している。

【０１０１】

先ず、データ送信装置２がデータを送信するまでの手順については、ステップＳ２１において、データ送信装置２は、データ受信装置３に伝送するＩＰデータグラムを、データ送信装置２自身又は双方向の通信経路９に繋がるインターフェースより、受け取る。インターネット６上からのアクセス情報に基づいて、情報センタの情報の提供を受け取る。

【０１０２】

次にステップＳ２２において、データ送信装置２は、ＩＰデータグラムの宛先アドレスを見て、第１のプロトコルの宛先アドレスを知る。例えば、データ送信装置２は、当該データ送信装置２内に所持している図８に示すようなＩＰアドレスとＭＡＣアドレスの対応表からデータ受信装置３の第１のプロトコルでの宛先アドレスを知る。

【０１０３】

そして、宛先アドレスを知ったデータ送信装置２は、その宛先アドレスをもとに上記セクションを作成する。ここで、データ送信装置２は、必要に応じてデータ部にビット１によるパディングを行い、データ部が６４ビットの倍数になるようにする。

【０１０４】

次に、ステップＳ２３において、例えば図６に示すようなＭＡＣアドレスとセッション鍵Ksの対応表から現在のセッション鍵Ksのフラグ１１２を見て、現在使用しているセッション鍵Ks２４を取り出し、当該取り出したセッション鍵Ksにより、上記図２中（ｃ）に示すように、セクションのデータ部を暗号化する。その際、現在のセッション鍵Ksのフラグを見て、その内容を上記図６に示すセッションのヘッダ部のｐｓｃ１１１の上位１ビットに入れる。

【０１０５】

次にステップＳ２４において、図２中（ｅ）乃至図２中（ｇ）に示すように、このセクション全体１０９を分割して各ＴＳパケット１０６，１０７，１０８のペイロード部Ｐに入れ、当該ＴＳパケット１０６，１０７，１０８に予め定められた上記ＰＩＤを付加し、さらに、第２のプロトコルの必要に応じてペイロード部Ｐを暗号化し、衛星回線４ａに送出する。

【０１０６】

以上がデータ送信装置２がデータを送信するまでの手順である。そして、データ受信装置３では、上述のようにして衛星回線４ａに送出されたデータを受信する。

【０１０７】

データ受信装置３は、先ず図９のステップＳ３１において、 衛星回線４ａより受信したＴＳパケット１０６，１０７，１０８を第２のプロトコルに従って復号化し、セクション全体１０９を再構築する。

【０１０８】

次に、ステップＳ３２において、データ受信装置３は、セクションの宛先アドレス（ＭＡＣアドレス）を取り出し、続いて、ステップＳ３３において、図１０に示すＭＡＣアドレスとセッション鍵Ksの対応表を参照してＭＡＣアドレスが存在するか否かの判別処理を行う。すなわち、自己に送信が許可されているデータを格納しているものであるか否かの判別処理を行う。ここで、ＭＡＣアドレスがないことを確認した場合には、データ受信装置３は、ステップＳ３４に進み、そのデータの破棄の処理を行う。また、ＭＡＣアドレスがあることを確認した場合には、データ送信装置３は、ステップＳ３５に進み、セクションヘッダ部１０３より上記図５に示すｐｓｃ１１１を取り出す。そして、データ送信装置３は、そのｐｓｃ１１１の上位１ビットから現在有効なセッション鍵Ksがどちらであるかを調べ、２つのセッション鍵Ksから現在有効とされるセッション鍵Ksを取り出す。

【０１０９】

データ受信装置３は、このようにして取り出したセッション鍵Ksにより、ステ

ップＳ３６において、セクションデータ部１０４をTriple-DESにより復号化する。　そして、データ受信装置３は、ステップＳ３７において、当該復号したデータからＩＰデータグラムを取り出す。例えば、ＩＰデータグラムの取り出しは、復号化されたデータ部の先頭にあるＩＰヘッダから図１１のTOTAL LENGTH フィールド１１３を読み取り、ＩＰデータグラムの長さを調べ、そこから計算されるＩＰデータグラム全体を取り出す。これにより、暗号化の際に付加した余計なパディングを除去される。このようにして目的とするＩＰデータグラムを取り出すことができる。

【０１１０】

以上のような手順により、データ送信装置２は、データを送信するまでの処理を行い、また、データ受信装置３は、受信したデータに対する処理を行い、自己に宛てて配信されてきた情報データを受け取る。

【０１１１】

このように構成されたデータ伝送システム１は、上述したように、各問題を解決することができる。

【０１１２】

なお、上記データ伝送システム１は、次のように変形することができる。第１の変形例であるデータ伝送システム２０１は、図１２に示すように構成される。このデータ伝送システム２０１は、データ受信装置３がＩＰルータとして構成される場合である。

【０１１３】

ところで、上述したデータ伝送システム１では、データ受信装置３ａが直接ＩＰデータグラムを受信する構成としている。しかし、このデータ伝送システム２０１では、データ受信装置３ａをＩＰルータとして構成することにより、データ受信装置３ａが衛星回線４ａから受信したデータを、イーサネットなどのローカルエリアネットワーク（ＬＡＮ）２０２を経由してつながっている衛星回線４ａへのインターフェースを持たないコンピュータ２０３ａ，２０３ｂにもデータを伝送することができる。その際、データ送信装置２やデータ受信装置３ａは、データ受信装置３ａだけでなく、それがつながっているローカルエリアネットワー

ク２０２上のコンピュータ２０３ａ，２０３ｂ全てについてのデータの限定受信制御を行うことができるようになる。具体的には、図８に示すデータ送信装置２内のＩＰアドレスとセクションの宛先アドレス（ＭＡＣアドレス）の対応表のＩＰアドレスが、個別のＩＰアドレスではなく、複数のＩＰアドレスの集合を示すＩＰのネットワークアドレスに変わることになる。但し、データ伝送システム２０１において、データ伝送を行うのは衛星回線４ａの区間のみであるため、データ受信装置３ａとコンピュータ２０３ａ，２０３ｂとの間でもデータ限定伝送制御を行うには、ＩＰプロトコル又はそれより上位のアプリケーションのレベルでのデータ限定伝送制御が必要となる。

【０１１４】

第２の変形例であるデータ伝送システム３０１は、図１３に示すように構成されている。このデータ伝送システム３０１では、データ受信装置３ａがブリッジとして構成され、ＩＰデータグラムを伝送するプロトコルの変換のみを行い、上記データ伝送システム２０１とでは、ルーティングを行わないことで異なる。

【０１１５】

上記データ受信装置３ａは、衛星回線４ａより受信したデータを復号化してＩＰデータグラムを取り出し、それをイーサネットフレームに入れて汎用のルータ３０２に転送する。そして、汎用のルータ３０２が、通常のＩＰデータグラムに対する処理を行う。これにより、ルーティングを行わないためにデータ受信装置３ａの構成が簡単になり、既存の汎用のルータを用いることができるようになる。

【０１１６】

【発明の効果】

本発明に係るデータ伝送制御方法は、データ送信手段からデータ受信手段へのデータの伝送に使用する第１の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、第１の通信経路よりもデータ伝送容量の小さく、データ受信手段からデータ送信手段へのデータの伝送にも使用される第２の通信経路、及び第１の通信経路の内の少なくとも第２の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行うことが

できる。

【０１１７】

このデータ伝送制御方法により、第１の通信経路及び第２の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第２の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行うことができる。

【０１１８】

よって、例えば、情報が各データ受信手段にデータが正しく伝わったかどうかをデータ送信手段が知ることができるようになる。

【０１１９】

本発明に係るデータ伝送システムは、データ送信手段からデータ受信手段へのデータの伝送に使用する第１の通信経路を介して、データ送信手段からデータ受信手段へのデータの送信を行い、少なくともデータ送信手段からデータ受信手段へのデータの伝送にも使用される通信経路であって、第１の通信経路よりもデータ伝送容量の小さい第２の通信経路を介して、データ送信手段及びデータ受信手段の間でデータ限定伝送制御情報の送信を行うことができる。

【０１２０】

これによりデータ伝送システムは、第１の通信経路及び第２の通信経路によりデータ送信手段からデータ受信手段へのデータ限定伝送制御情報を含むデータの送信を行うとともに、第２の通信経路により当該データ送信手段と当該データ受信手段との間でのデータの送受信に関する情報に関して情報の交換を行うことができる。

【０１２１】

よって、例えば、情報が各データ受信手段にデータが正しく伝わったかどうかをデータ送信手段が知ることができるようになる。

【０１２２】

また、本発明に係るデータ伝送制御方法は、データ送信手段からデータ受信手段に送信されるデータが複数のプロトコルによって多重化してカプセル化できる

。

【０１２３】

これにより、所定のプロトコルを保ったままデータの送信が可能になり、すなわち、例えば、所定のプロトコルとの互換性を保ったままデータの送信が可能になり、さらに、所定のデータを格納するための空間が確保することができるプロトコルによりカプセル化することにより、各種情報を格納するためのデータ空間を確保することができる。さらに、暗号化が施されることにより、データの安全性を保することができる。

【０１２４】

例えば、所定のデータを収納することができるプロトコルによってカプセル化することにより、暗号鍵等の宛先アドレスに関する情報を格納するための空間を十分に確保することができ、従来のＴＳパケット方式を採用したときにＰＩＤ部及びスクランブル制御部に格納していたときよりも宛先アドレスに関する情報を増加させることができる。これにより、ＰＩＤ部を増加させなくて済む。

【０１２５】

また、例えば、アプリケーション毎に制御方法を用意しなくて済み、新しいアプリケーションへの素早い対応ができるようになる。また、認証ヘッダや暗号ペイロードを既存のインターネットで使うことができるようになる。

【０１２６】

また、本発明に係るデータ伝送制御方法は、データ暗号工程において暗号鍵により暗号化されたデータに当該データの暗号化に使用した暗号鍵に関する暗号鍵情報を付加して、データ送信工程により、データ送信手段からデータ受信手段へ当該データを送信することができる。そして、データ受信手段において、データ復号化工程により、受信した暗号化されたデータを復号するための複数の復号鍵であって、頻繁に更新される復号鍵から、暗号化されたデータに付加されている暗号鍵情報に基づいて選択した一つの復号鍵により、当該暗号化されたデータの復号化を行うことができる。

【０１２７】

このデータ伝送制御方法により、データ送信手段は、暗号鍵によるデータの暗

号化を行い、データ受信手段は、受信した暗号化されているデータを復号鍵により復号化することができる。さらに、データ受信手段は、頻繁に変更される復号鍵から一つの復号鍵を選択して、当該選択した復号鍵により復号化を行うことができる。このとき、データ受信手段は、当該暗号化されたデータとともに送信されてくる暗号鍵情報に基づいて複数の復号鍵から一つの復号鍵を選択する。

【図面の簡単な説明】

【図１】

本発明の実施の形態であるデータ伝送システムの構成を示す図である。

【図２】

上記データ伝送システムを構成するデータ送信装置からデータ受信装置へ送信されるデータであって、複数のプロトコルによってカプセル化が施されたデータを示す図である。

【図３】

上記データ送信装置及び上記データ受信装置の構成を示すブロック図である。

【図４】

上記データ送信装置から上記データ受信装置へ送信されるデータを暗号化するセッション鍵の変更を行う手続きの一連の工程を示すフローチャートである。

【図５】

セクションヘッダのデータ構造を示す図である。

【図６】

ＭＡＣアドレスとセッション鍵Ksのフラグとの対応表を示す図である。

【図７】

上記データ送信装置において行うデータのカプセル化の一連の手続きを示すフローチャートである。

【図８】

ＩＰアドレスとＭＡＣアドレスとの対応表を示す図である。

【図９】

上記データ受信装置が受信したデータをセッション鍵Ksにより復号化するときの一連の手続きを示すフローチャートである。

【図１０】

ＭＡＣアドレスとセッション鍵Ksの対応表を示す図である。

【図１１】

ＩＰデータグラムの取り出しの際に使用されるTOTALLENGTHフィールドが格納されるデータ構造を示す図である。

【図１２】

上記データ伝送システムの第１の変形例を示す図である。

【図１３】

上記データ伝送システムの第２の変形例を示す図である。

【図１４】

従来のデータ伝送システムの構成を説明するために用いた図である。

【図１５】

上記従来のデータ伝送システムにおいてデータを伝送するためのイーサネットフレームのデータ構造であって、宛先アドレスが格納されているイーサネットフレームのデータ構造を示す図である。

【図１６】

従来のデータ伝送システムにおいて、イーサネットを介して受信したイーサフレームに自己の宛先アドレスが格納されているか否か、さらにその判断に基づいて行う処理についての一連の手続きを示すフローチャートである。

【図１７】

ＴＳパケットのデータ構造のフォーマットを示す図である。

【図１８】

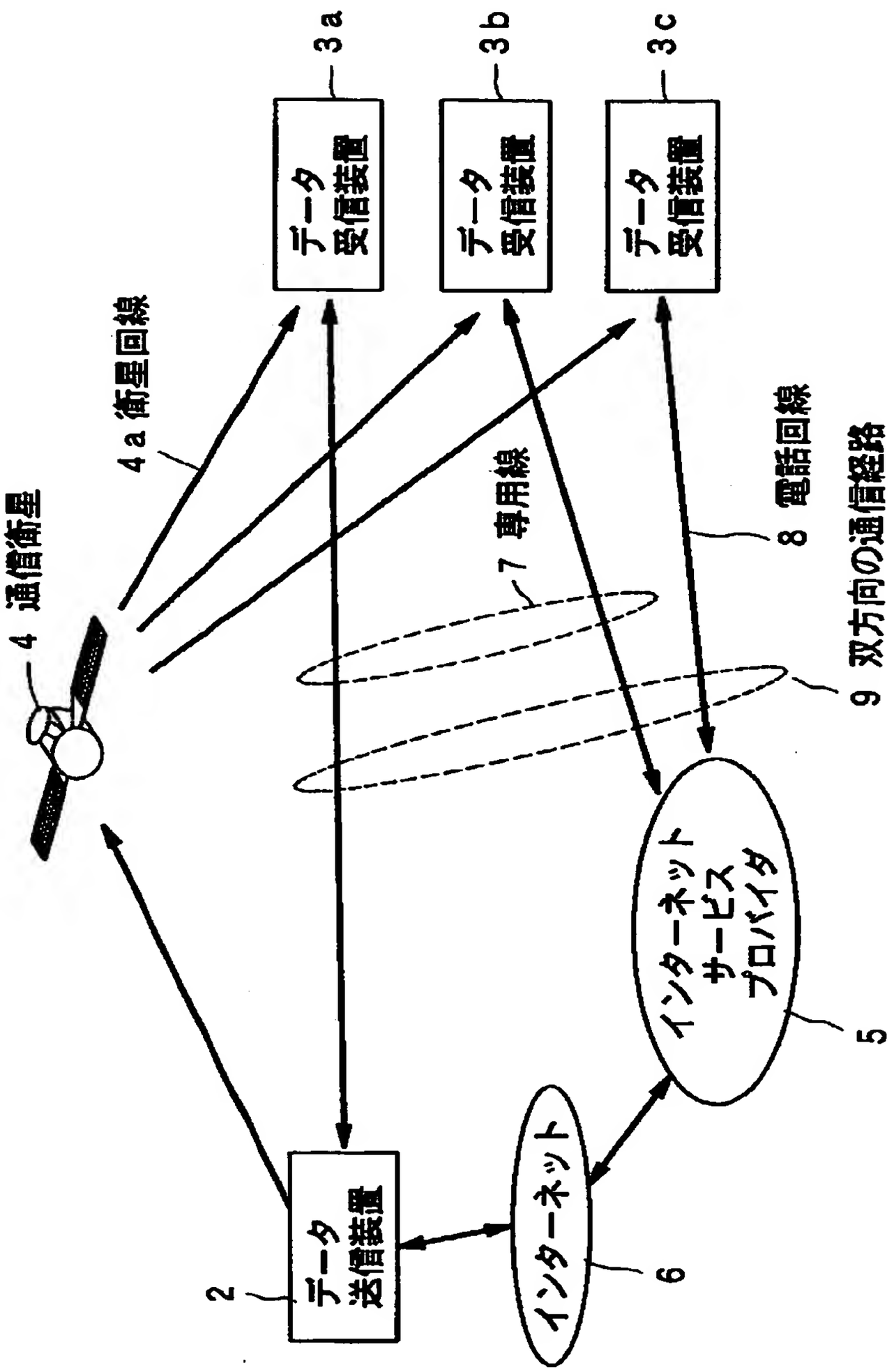
従来のデータ伝送システムを構成するデータ送信装置及びデータ受信装置の構成を示す図である。

【符号の説明】

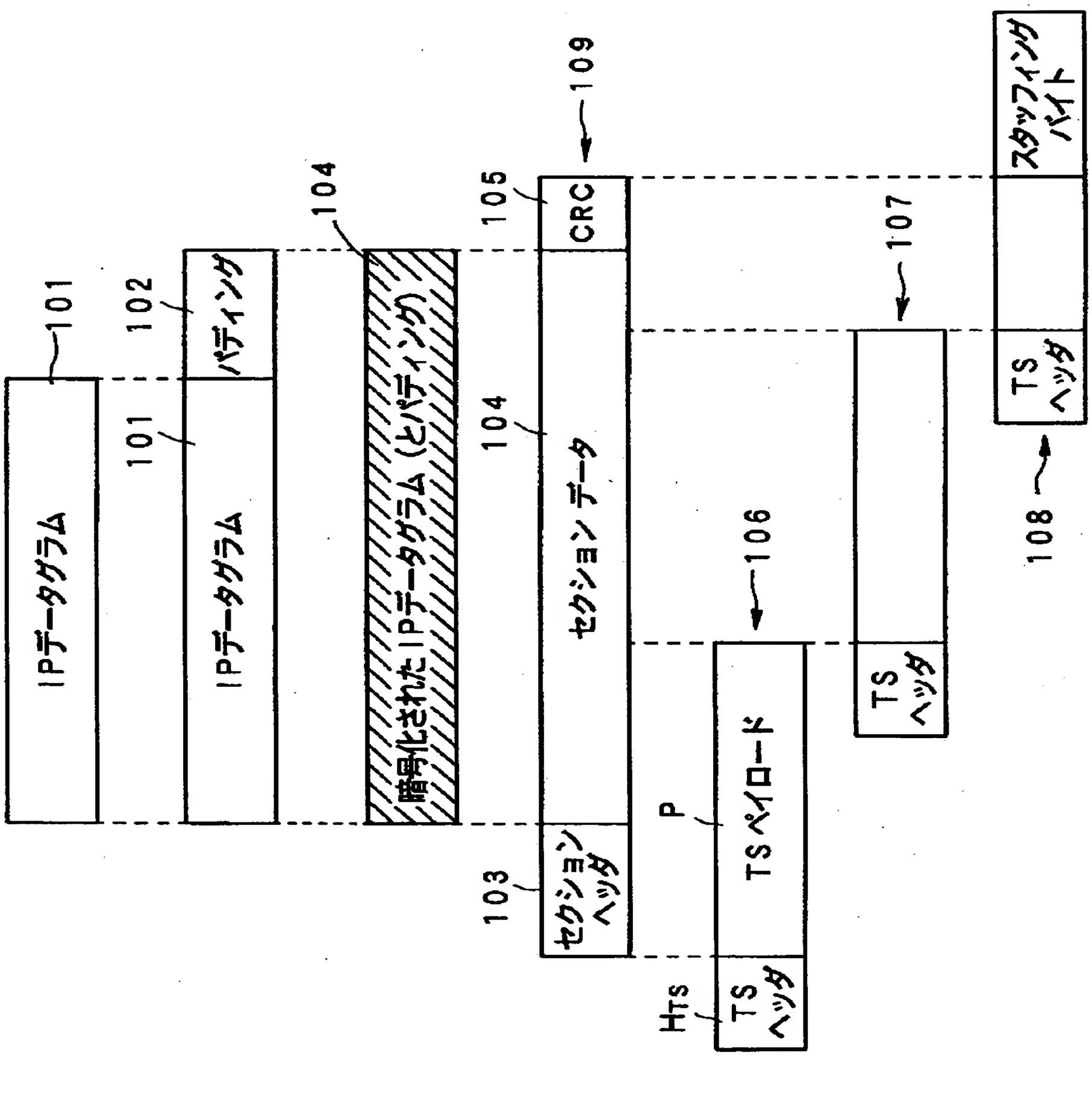
１　データ伝送システム 、２　データ送信装置、３　データ受信装置、４　通信衛星、４ａ　衛星回路、７　専用線、８　電話回線、９　双方向の通信回線、２４　セッション鍵、２５　マスター鍵

【書類名】　図面

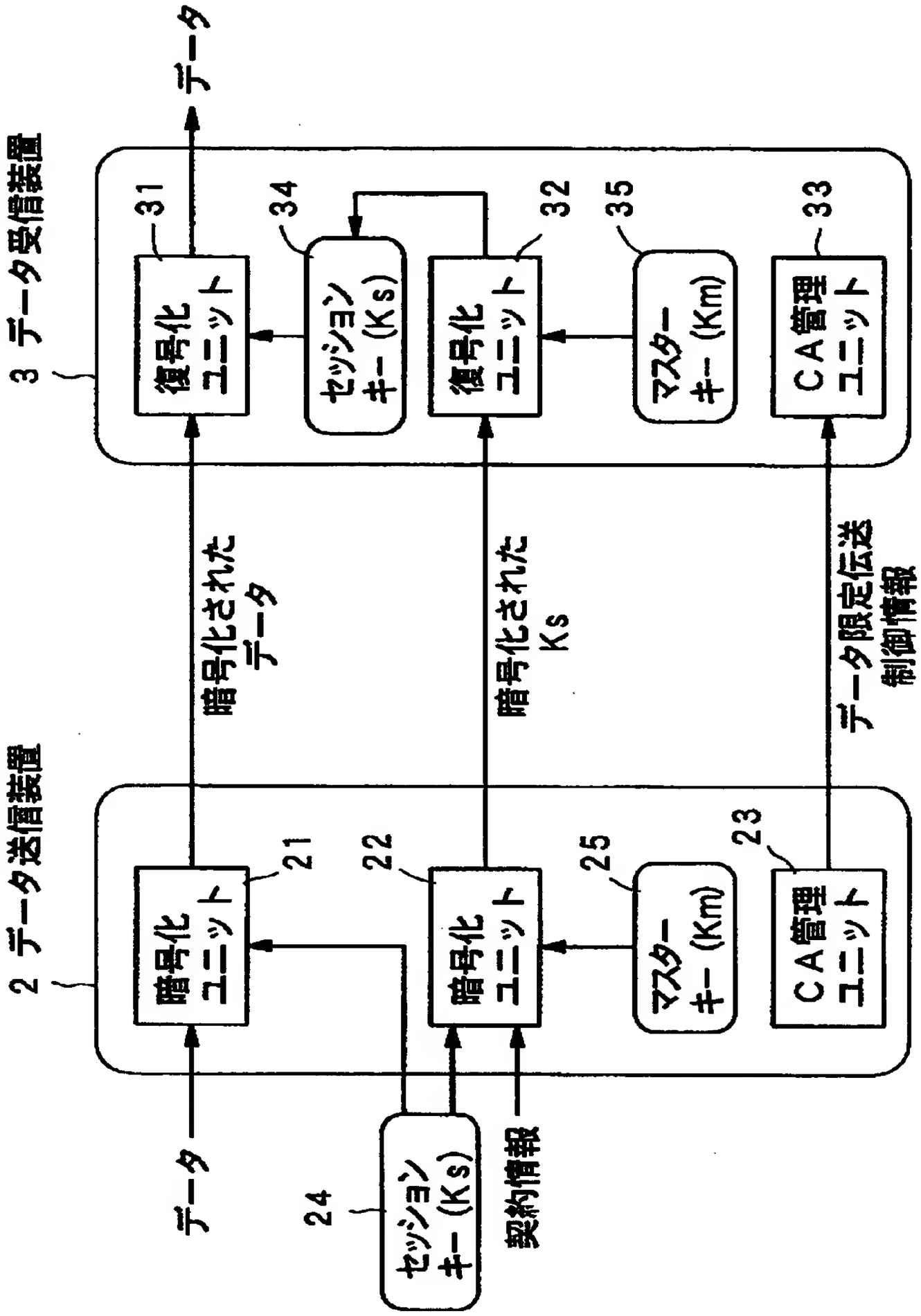
【図１】


3a
データ
受信装置
3b
データ
受信装置
3c
データ
受信装置
4a 衛星回線
4 通信衛星
7 専用線
8 電話回線
9 双方向の通信経路
インターネット
サービス
プロバイダ
5
1 データ伝送システム
2
データ
送信装置
インターネット
6

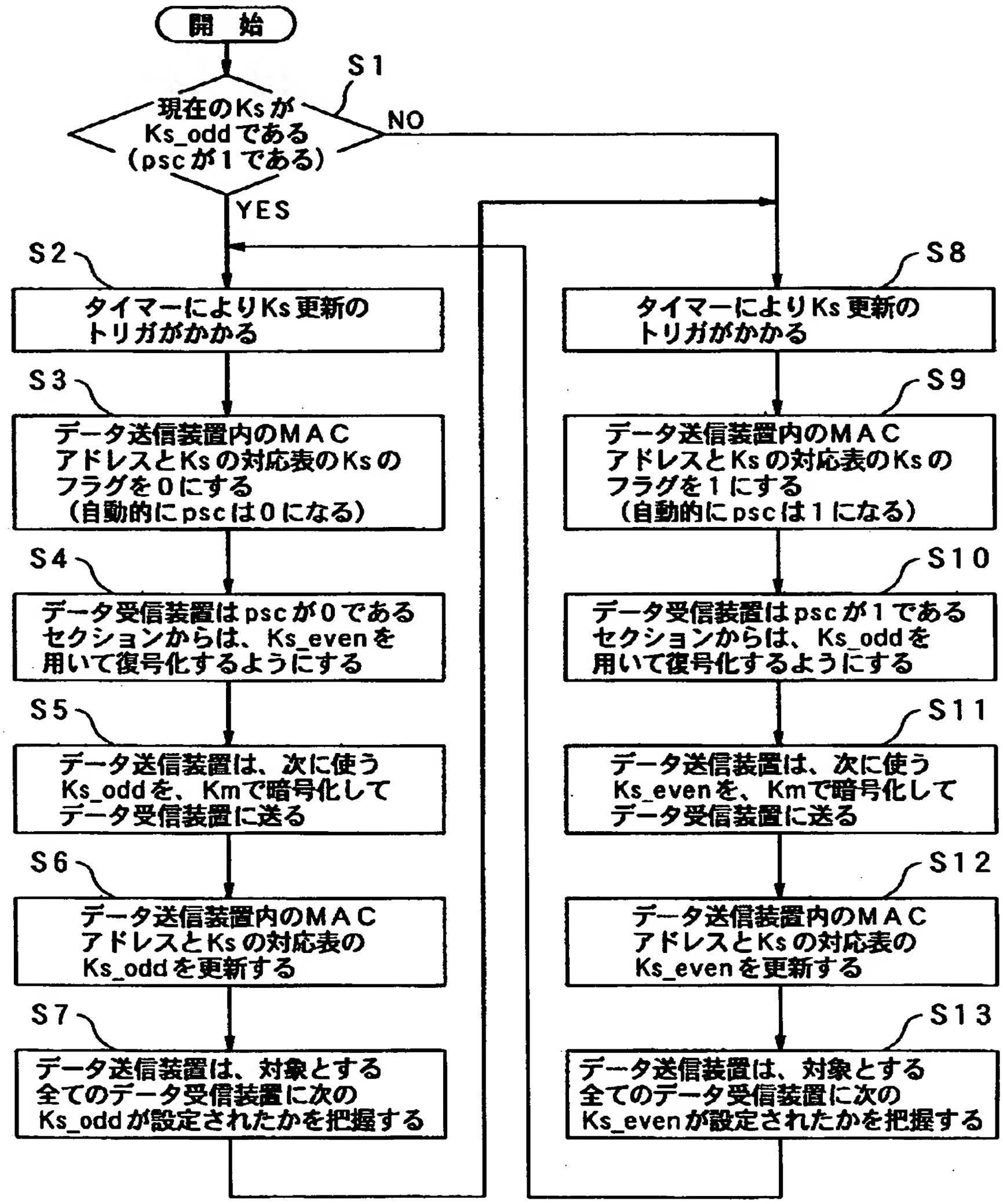
【図２】


101
IPデータグラム
102
パディング
101
IPデータグラム
暗号化されたIPデータグラム（とパディング）
104
セクション データ
105
CRC
109
スタッフィング バイト
107
TS ヘッダ
108
TS ヘッダ
104
セクション ヘッダ
103
106
P
TS ペイロード
HTS
TS ヘッダ
(a)
(b)
(c)
(d)
(e)
(f)
(g)

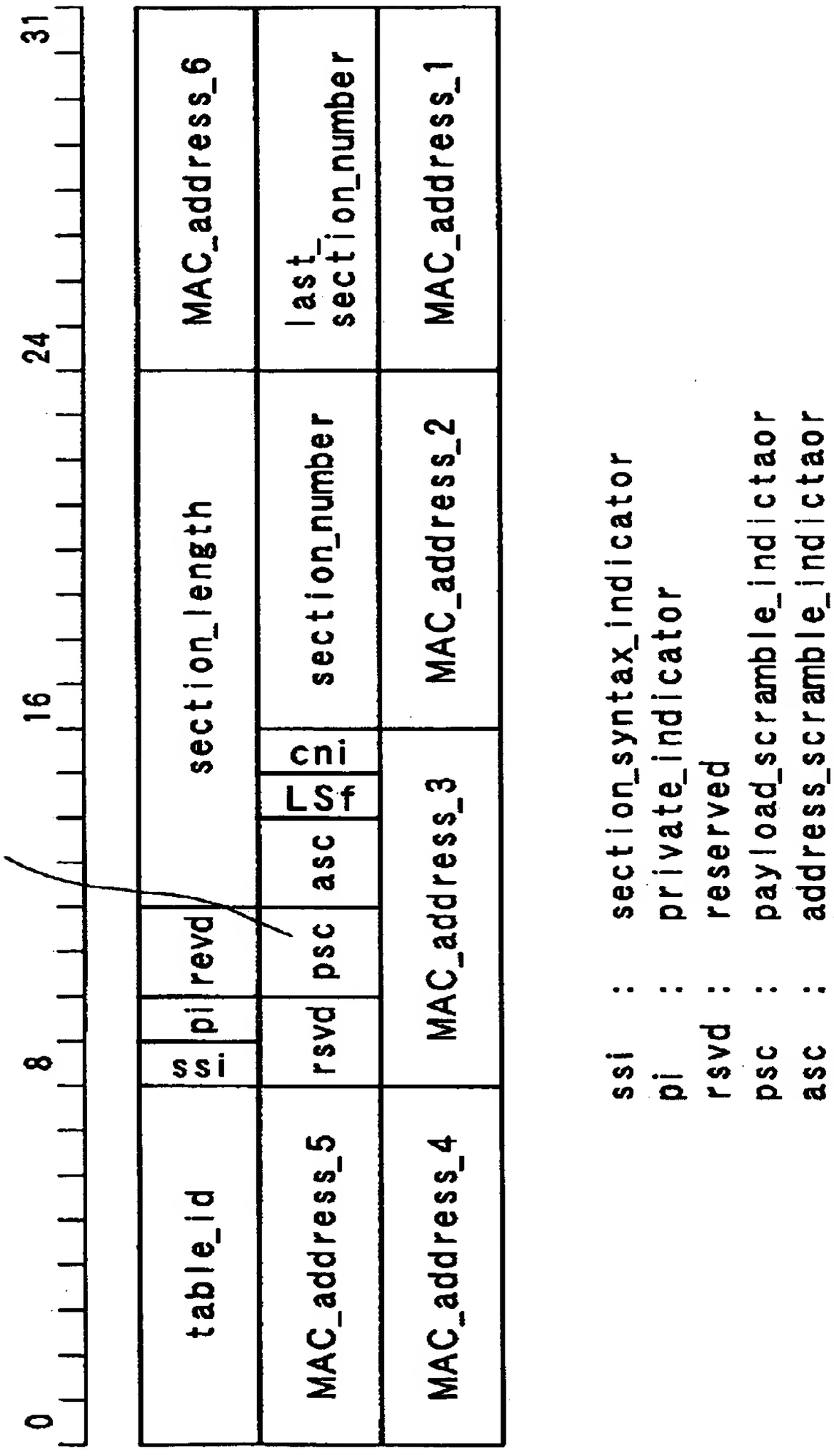
【図３】


データ
3 データ受信装置
31
復号化ユニット
34
セッションキー (Ks)
32
復号化ユニット
35
マスターキー (Km)
33
CA管理ユニット
暗号化されたデータ
暗号化されたKs
データ限定伝送制御情報
2 データ送信装置
21
暗号化ユニット
22
暗号化ユニット
25
マスターキー (Km)
23
CA管理ユニット
データ
24
セッションキー (Ks)
契約情報

【図４】


開　始
S1
現在のKsが
Ks_oddである
（pscが１である）
NO
YES
S2
タイマーによりKs更新の
トリガがかかる
S3
データ送信装置内のＭＡＣ
アドレスとKsの対応表のKsの
フラグを０にする
（自動的にpscは０になる）
S4
データ受信装置はpscが０である
セクションからは、Ks_evenを
用いて復号化するようにする
S5
データ送信装置は、次に使う
Ks_oddを、Kmで暗号化して
データ受信装置に送る
S6
データ送信装置内のＭＡＣ
アドレスとKsの対応表の
Ks_oddを更新する
S7
データ送信装置は、対象とする
全てのデータ受信装置に次の
Ks_oddが設定されたかを把握する
S8
タイマーによりKs更新の
トリガがかかる
S9
データ送信装置内のＭＡＣ
アドレスとKsの対応表のKsの
フラグを１にする
（自動的にpscは１になる）
S10
データ受信装置はpscが１である
セクションからは、Ks_oddを
用いて復号化するようにする
S11
データ送信装置は、次に使う
Ks_evenを、Kmで暗号化して
データ受信装置に送る
S12
データ送信装置内のＭＡＣ
アドレスとKsの対応表の
Ks_evenを更新する
S13
データ送信装置は、対象とする
全てのデータ受信装置に次の
Ks_evenが設定されたかを把握する

【図５】

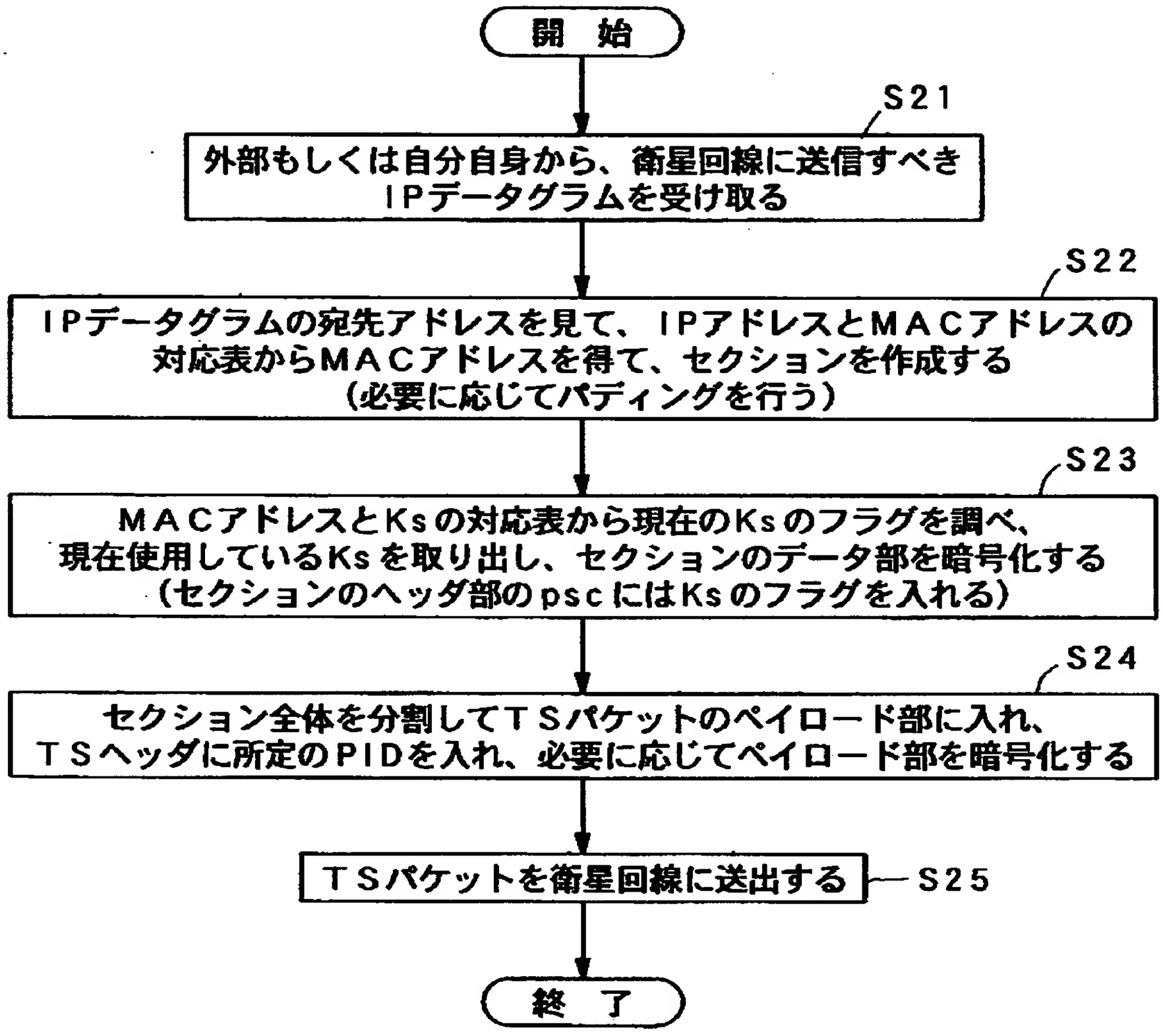

31
24
16
8
0
111
table_id
section_length
MAC_address_6
MAC_address_5
MAC_address_4
MAC_address_3
MAC_address_2
MAC_address_1
ssi
pi
revd
rsvd
psc
asc
LSf
cni
section_number
last_section_number
ssi : section_syntax_indicator
pi : private_indicator
rsvd : reserved
psc : payload_scramble_indictaor
asc : address_scramble_indictaor
LSf : LLC_SNAP_flag
cni : current_next_indicator

【図６】

112

MACアドレス	Ks_even	Ks_odd	Ksフラグ
08:00:46:01:07:24	0xC08F...25	0x90B3...AF	0
08:00:46:01:07:09	0x26D2...61	0xBA02...3C	1
01:00:5e:16:0:0	0x461E...67	0xDC1A...22	0

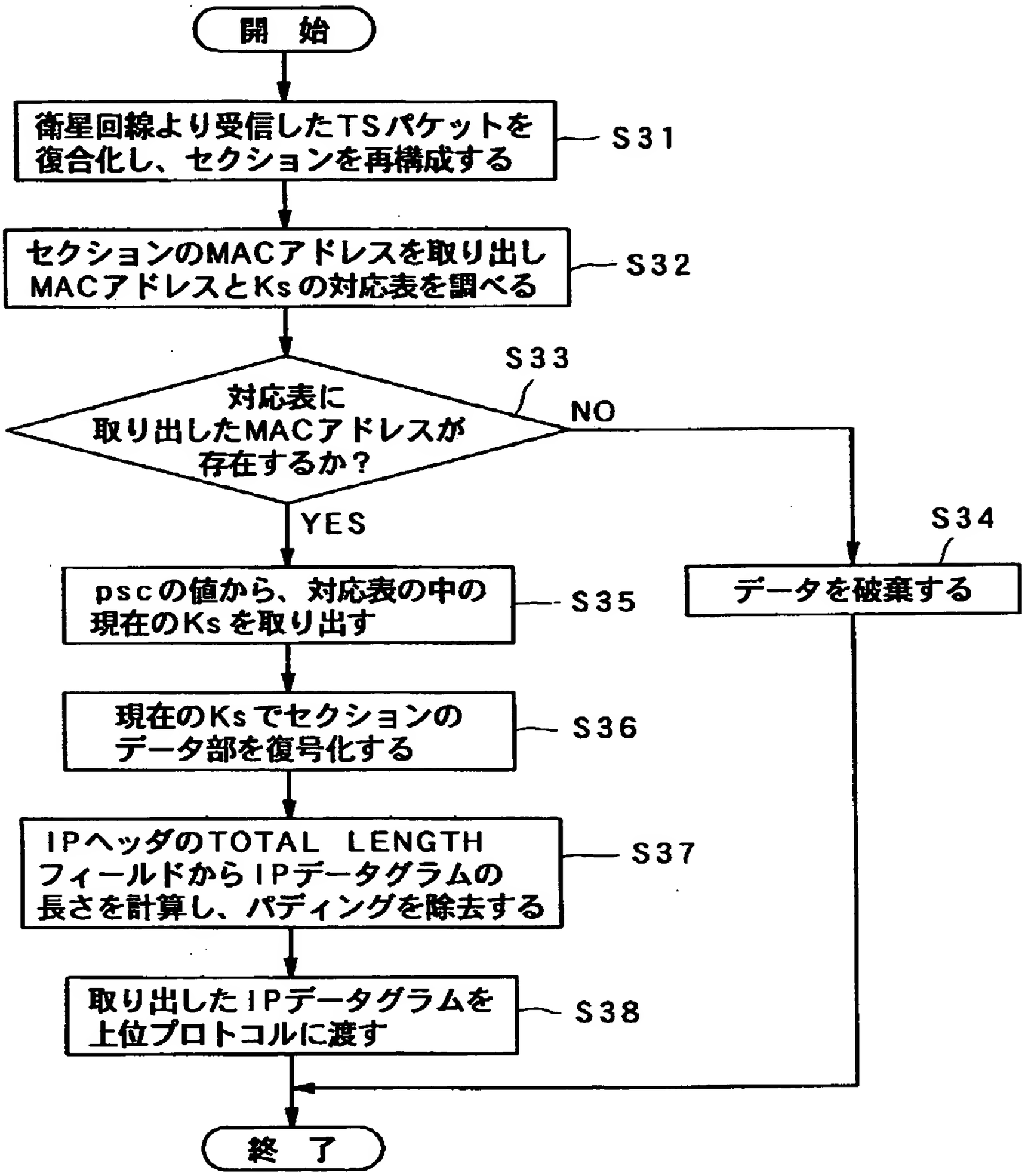
【図７】


開　始
S21
外部もしくは自分自身から、衛星回線に送信すべき
IPデータグラムを受け取る
S22
IPデータグラムの宛先アドレスを見て、IPアドレスとＭＡＣアドレスの
対応表からＭＡＣアドレスを得て、セクションを作成する
（必要に応じてパディングを行う）
S23
ＭＡＣアドレスとKsの対応表から現在のKsのフラグを調べ、
現在使用しているKsを取り出し、セクションのデータ部を暗号化する
（セクションのヘッダ部のpscにはKsのフラグを入れる）
S24
セクション全体を分割してＴＳパケットのペイロード部に入れ、
ＴＳヘッダに所定のＰＩＤを入れ、必要に応じてペイロード部を暗号化する
ＴＳパケットを衛星回線に送出する
S25
終　了

【図８】

IPアドレス	bitmask	MAC address
133. 11. 9. 39	255. 255. 255. 225	08:00:46:01:07:24
133. 11. 20. 0	255. 255. 255. 0	08:00:46:01:07:09
226. 0. 0. 0	255. 255. 255. 224	01:00:5e:16:0:0

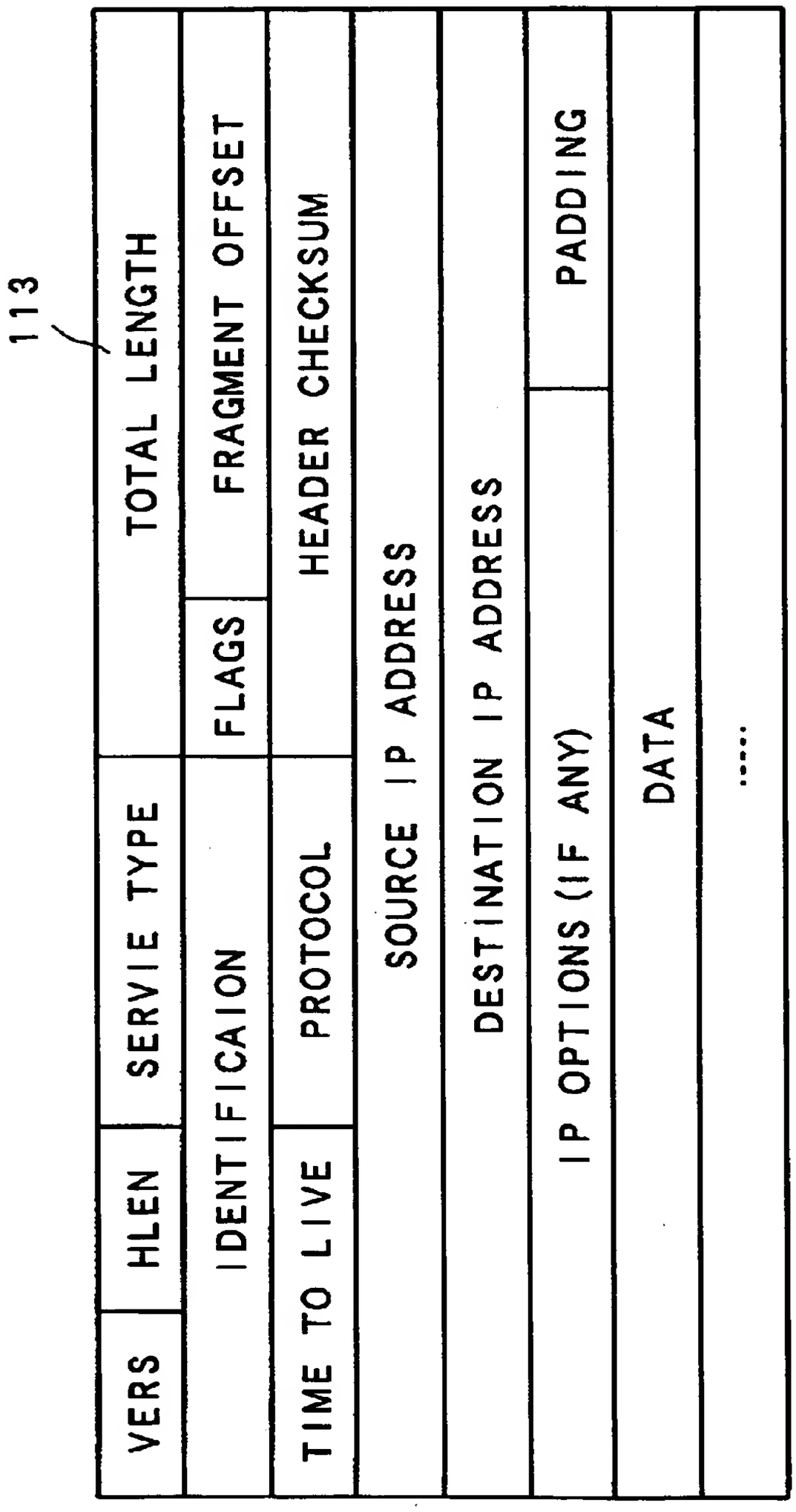
【図９】


開　始
衛星回線より受信したTSパケットを
復合化し、セクションを再構成する
S31
セクションのMACアドレスを取り出し
MACアドレスとKsの対応表を調べる
S32
S33
対応表に
取り出したMACアドレスが
存在するか？
NO
YES
S34
データを破棄する
pscの値から、対応表の中の
現在のKsを取り出す
S35
現在のKsでセクションの
データ部を復号化する
S36
IPヘッダのTOTAL LENGTH
フィールドからIPデータグラムの
長さを計算し、パディングを除去する
S37
取り出したIPデータグラムを
上位プロトコルに渡す
S38
終　了

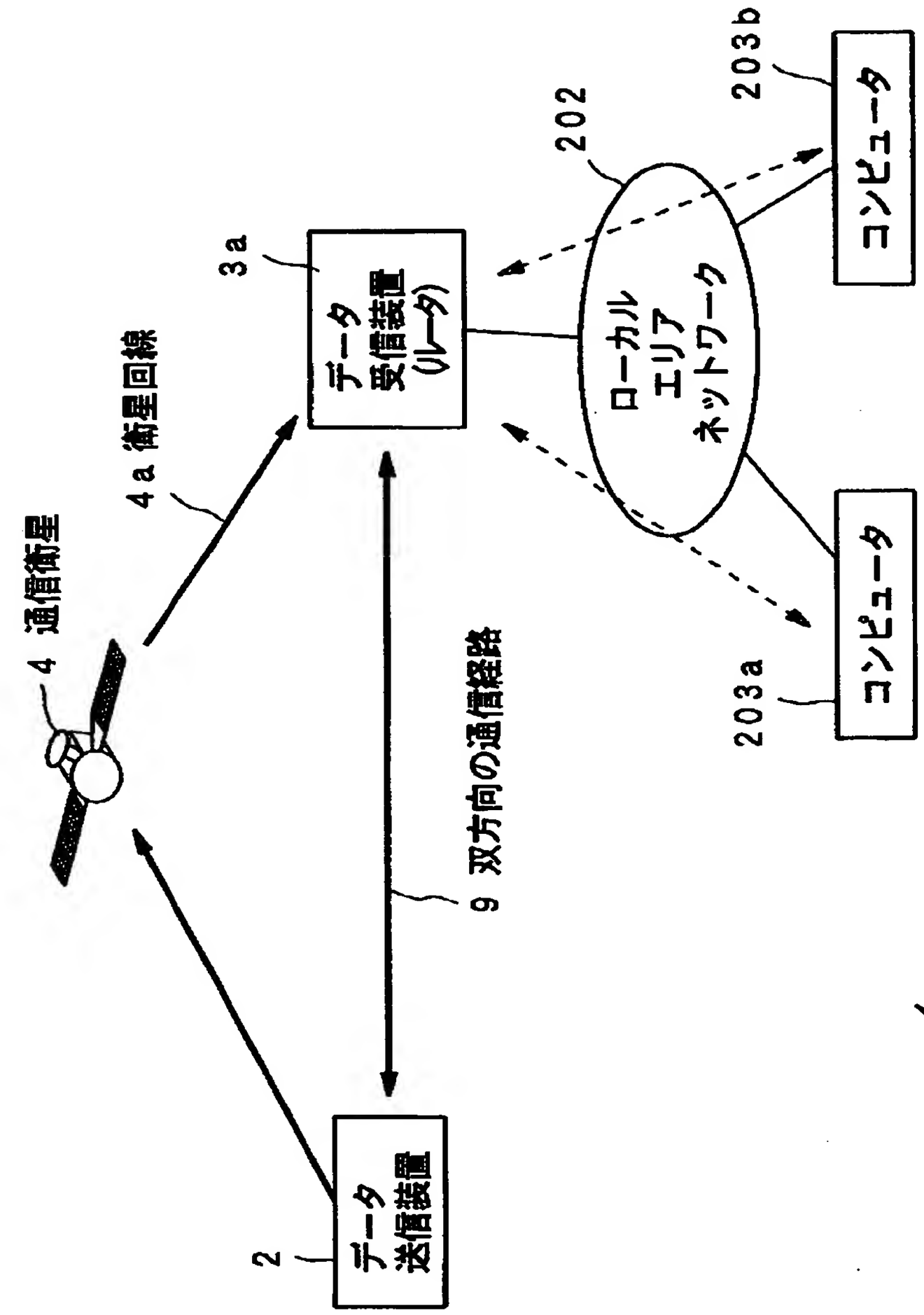
【図１０】

MACアドレス	Ks_even	Ks_odd
08:00:46:01:07:24	0xC08F...25	0x90B3...AF
01:00:5e:16:0:0	0x461E...67	0xDC1A...22

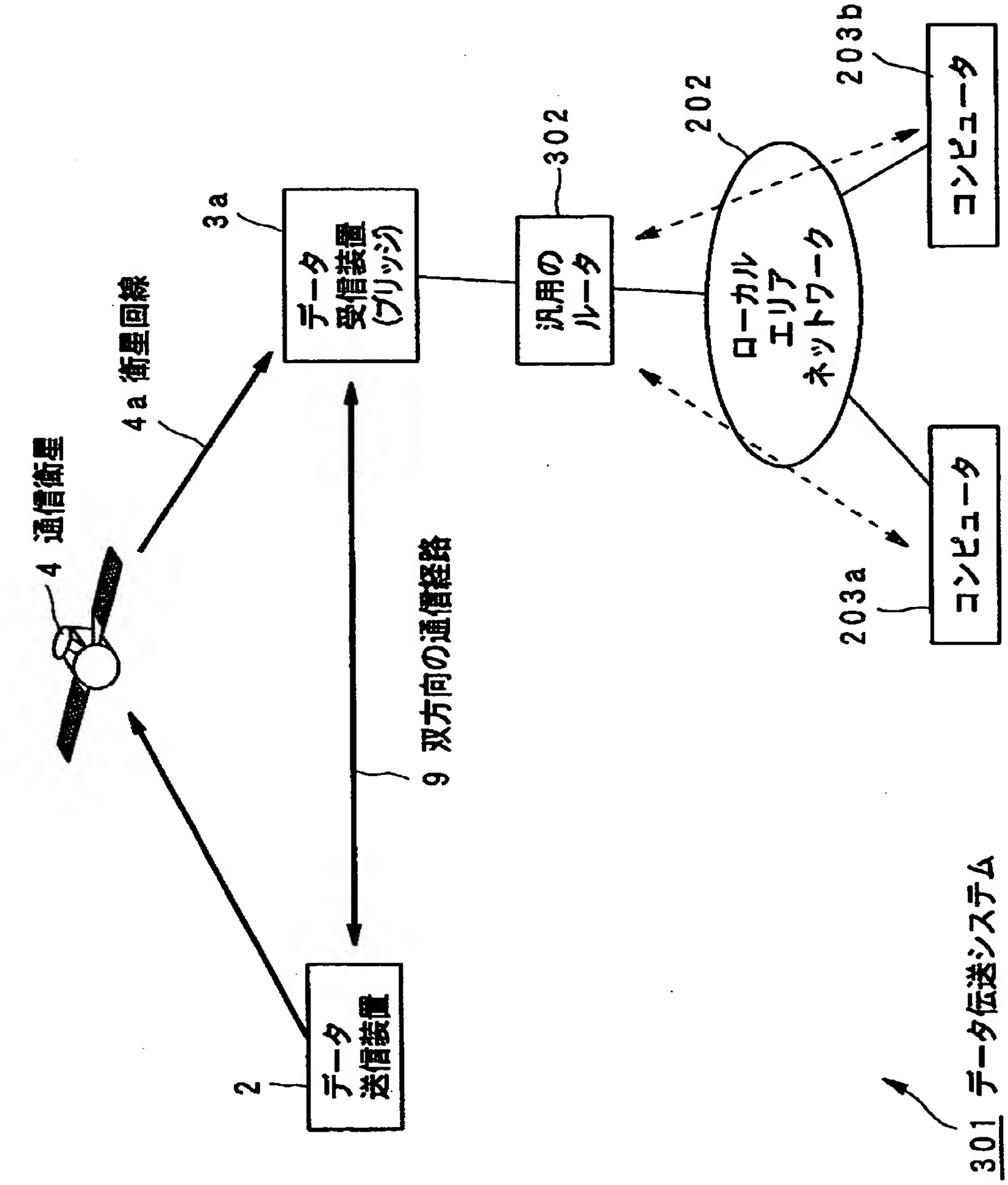
【図１１】


113
VERS
HLEN
SERVIE TYPE
TOTAL L
IDENTIFICAION
FLAGS
FRAGM
TIME TO LIVE
PROTOCOL
HEADER C
SOURCE IP ADDRESS
DESTINATION IP ADDRESS
IP OPTIONS (IF ANY)
PADDING
DATA
.....

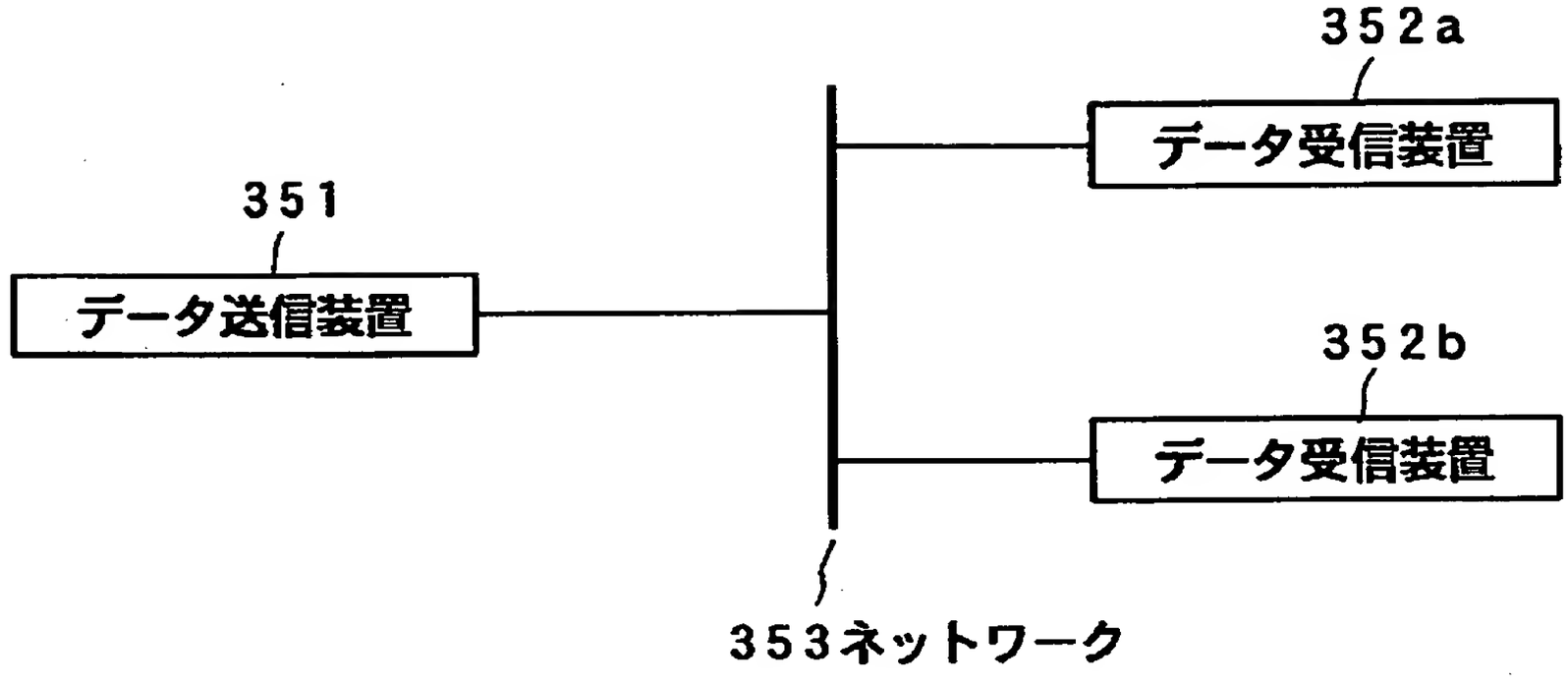
【図１２】


201 データ伝送システム
4 通信衛星
4a 衛星回線
9 双方向の通信経路
2 データ送信装置
3a データ受信装置(リータ)
202 ローカルエリアネットワーク
203a コンピュータ
203b コンピュータ

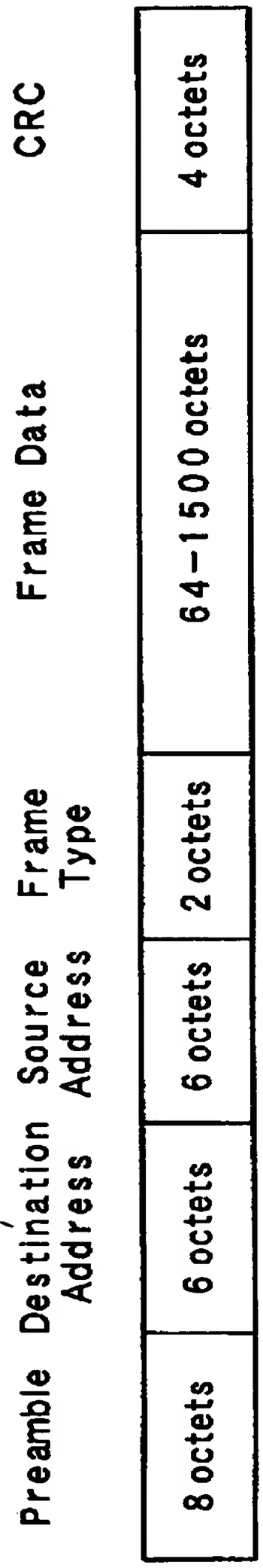
【図１３】


データ伝送システム
301
データ
送信装置
2
4 通信衛星
4a 衛星回線
データ
受信装置
(プリッジ)
3a
9 双方向の通信経路
汎用の
ルータ
302
ローカル
エリア
ネットワーク
202
コンピュータ
203a
コンピュータ
203b

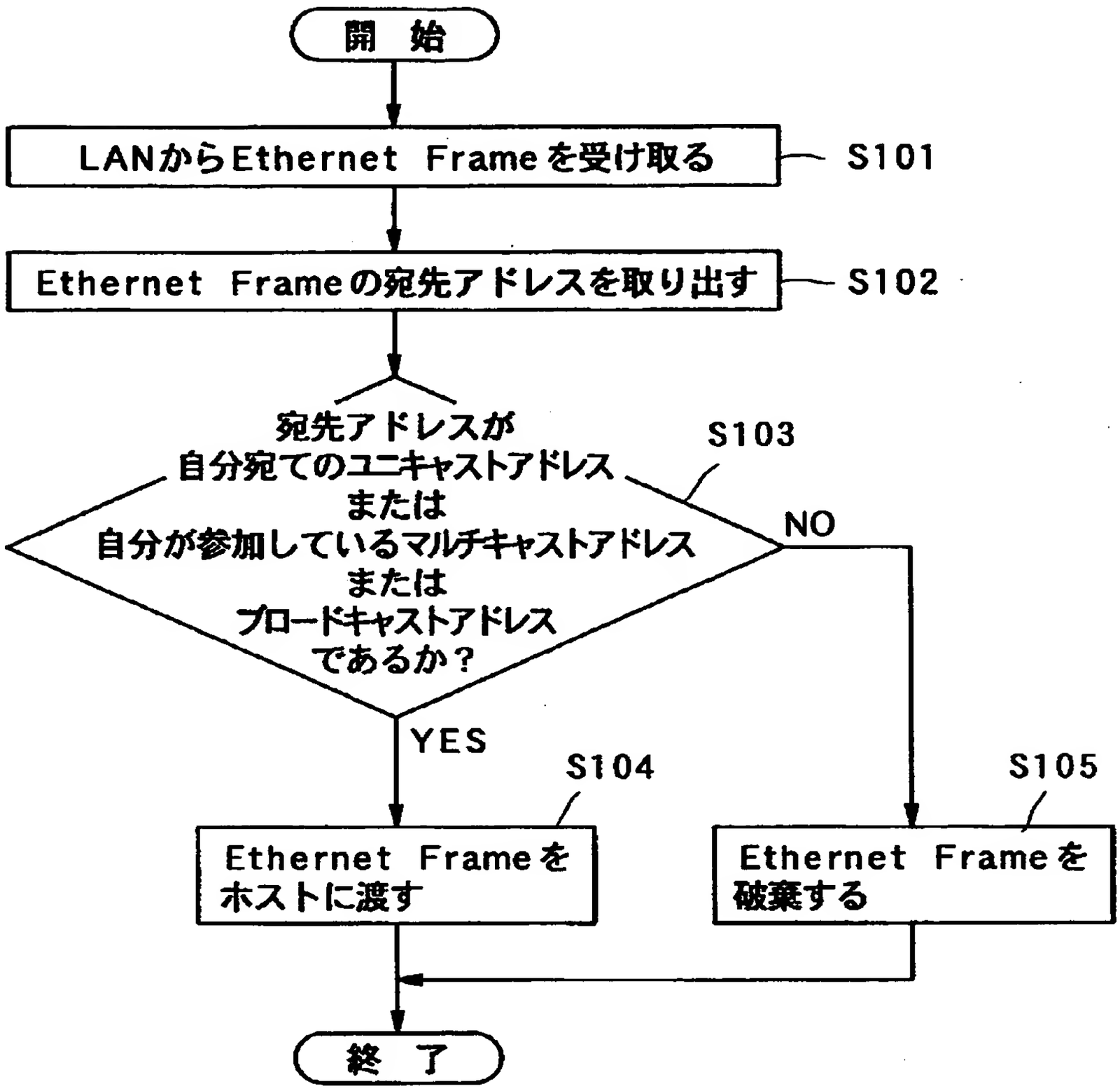
【図１４】



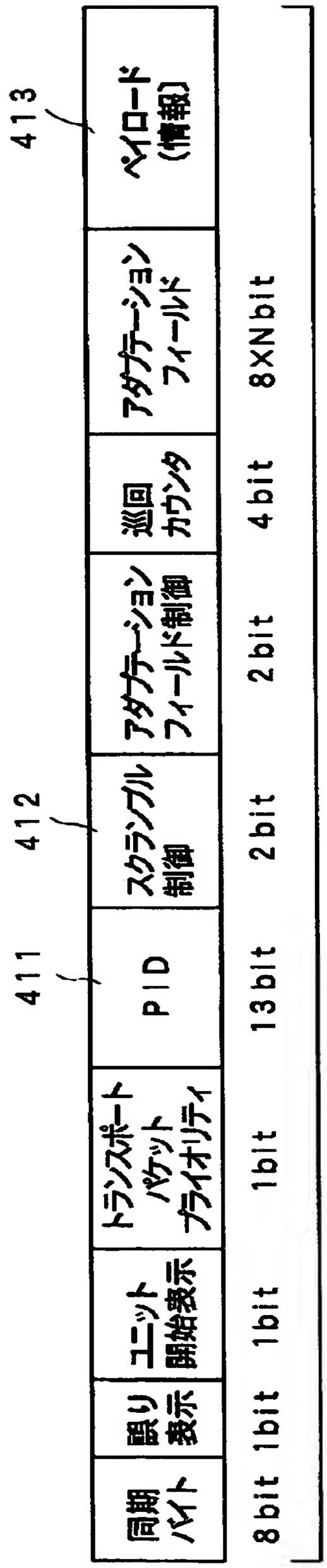
【図１５】


401
Preamble
8 octets
Destination Address
6 octets
Source Address
6 octets
Frame Type
2 octets
Frame Data
64－1500 octets
CRC
4 octets

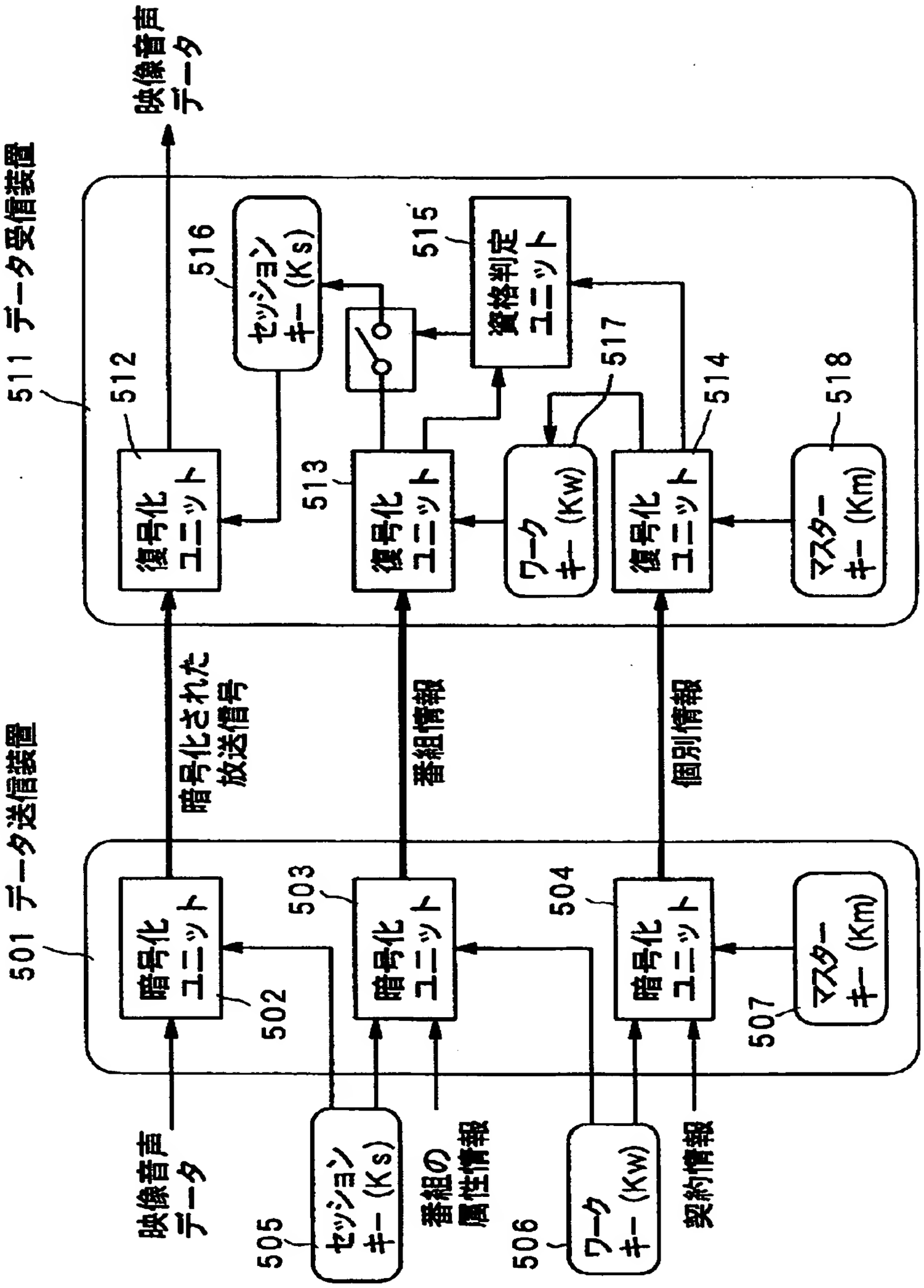
【図１６】


開　始
LANからEthernet　Frameを受け取る
S101
Ethernet　Frameの宛先アドレスを取り出す
S102
宛先アドレスが
自分宛てのユニキャストアドレス
または
自分が参加しているマルチキャストアドレス
または
ブロードキャストアドレス
であるか？
S103
NO
YES
S104
Ethernet　Frameを
ホストに渡す
S105
Ethernet　Frameを
破棄する
終　了

【図１７】


413
ペイロード（情報）
アダプテーションフィールド
8×N bit
411
412
PID
スクランブル制御
アダプテーションフィールド制御
巡回カウンタ
13bit
2bit
2bit
4bit
188byte
同期バイト
誤り表示
ユニット開始表示
トランスポートパケットプライオリティ
8bit
1bit
1bit
1bit

【図１８】


映像音声データ
501 データ送信装置
暗号化ユニット
502
503
504
507
マスターキー (Km)
セッションキー (Ks)
505
番組の属性情報
ワークキー (Kw)
506
契約情報
暗号化された放送信号
番組情報
個別情報
511 データ受信装置
512
513
514
518
復号化ユニット
516
515
資格判定ユニット
517

【書類名】　　要約書

【要約】

【課題】　データ送信装置からデータ受信装置へのデータの送信を安全に、さらに確実に行うことを実現可能にするデータ伝送システムの提供を目的とする。

【解決手段】　データ伝送システム１は、暗号化を施してデータを送信するデータ送信装置２と、データ送信装置２から暗号化が施されたデータが配信されるデータ受信装置３ａ，３ｂ，３ｃと、データ送信装置２からデータ受信装置３ａ，３ｂ，３ｃへのデータの伝送に使用する衛星回線４ａと、データ受信装置３ａ，３ｂ，３ｃからデータ送信装置２へのデータの伝送にも使用され、衛星回線４ａよりもデータ伝送容量の小さい双方向の通信経路９とを有し、データ送信装置２からデータ受信装置３ａ，３ｂ，３ｃへの暗号化したデータの伝送には、衛星回線４ａを用い、データ送信装置２とデータ受信装置３ａ，３ｂ，３ｃとの間のデータ限定伝送制御情報の通信には、少なくとも双方向の通信経路９を用いる。

【選択図】　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000002185
【住所又は居所】　東京都品川区北品川６丁目７番３５号
【氏名又は名称】　ソニー株式会社
【代理人】　申請人
【識別番号】　100067736
【住所又は居所】　東京都港区虎ノ門２－６－４　第１１森ビル　小池国際特許事務所
【氏名又は名称】　小池　晃
【選任した代理人】
【識別番号】　100086335
【住所又は居所】　東京都港区虎ノ門２丁目６番４号　第１１森ビル小池国際特許事務所
【氏名又は名称】　田村　榮一
【選任した代理人】
【識別番号】　100096677
【住所又は居所】　東京都港区虎ノ門二丁目６番４号　第１１森ビル小池国際特許事務所
【氏名又は名称】　伊賀　誠司

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社